Wi-Fi en entreprise : Application et Sécurité

Benjamin CHARLES

20 février 2007

benjamin [at] polkaned [dot] net

Plan

- Concepts
- Mise en œuvre
- Analyse de la sécurité

Plan

- **Concepts**
- Mise en œuvre
- Analyse de la sécurité

Concepts
2 familles d'équipements

FAT AP

LIGHT AP & Wireless Controller

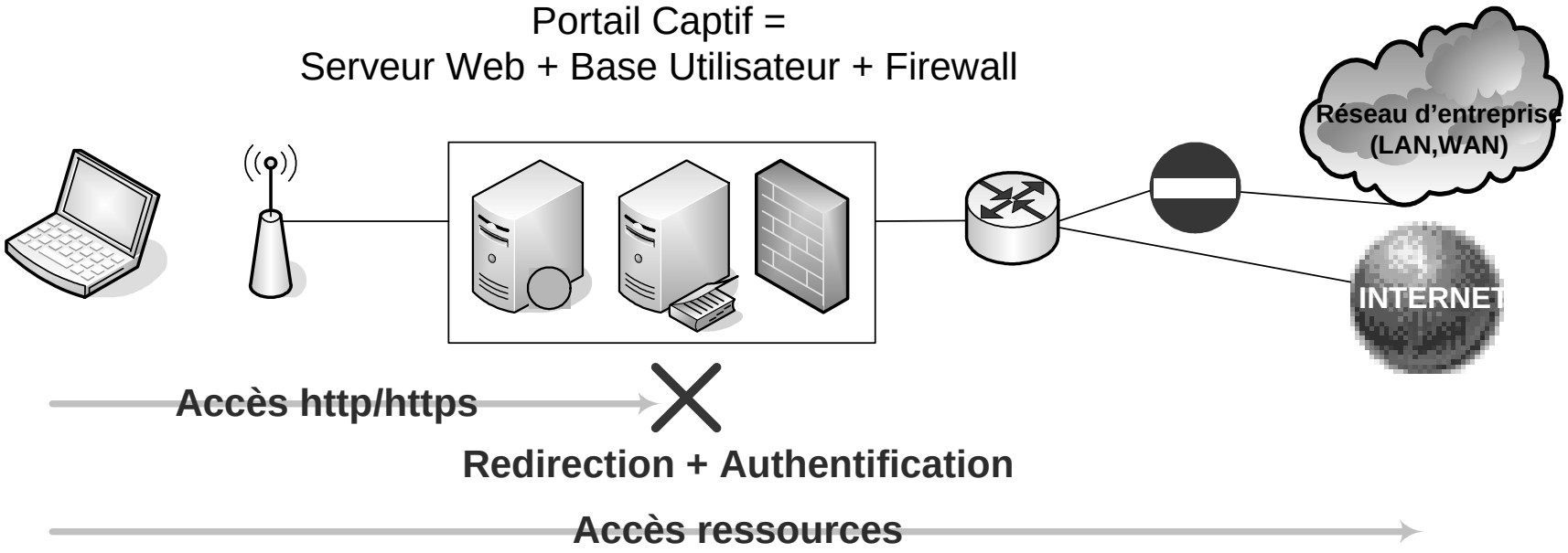
Concepts
Fonctionnalités

- Gestion de la radio
- Routeur
- Firewall
- Portail captif
- AAA
- IDS/IPS
- Géo-localisation

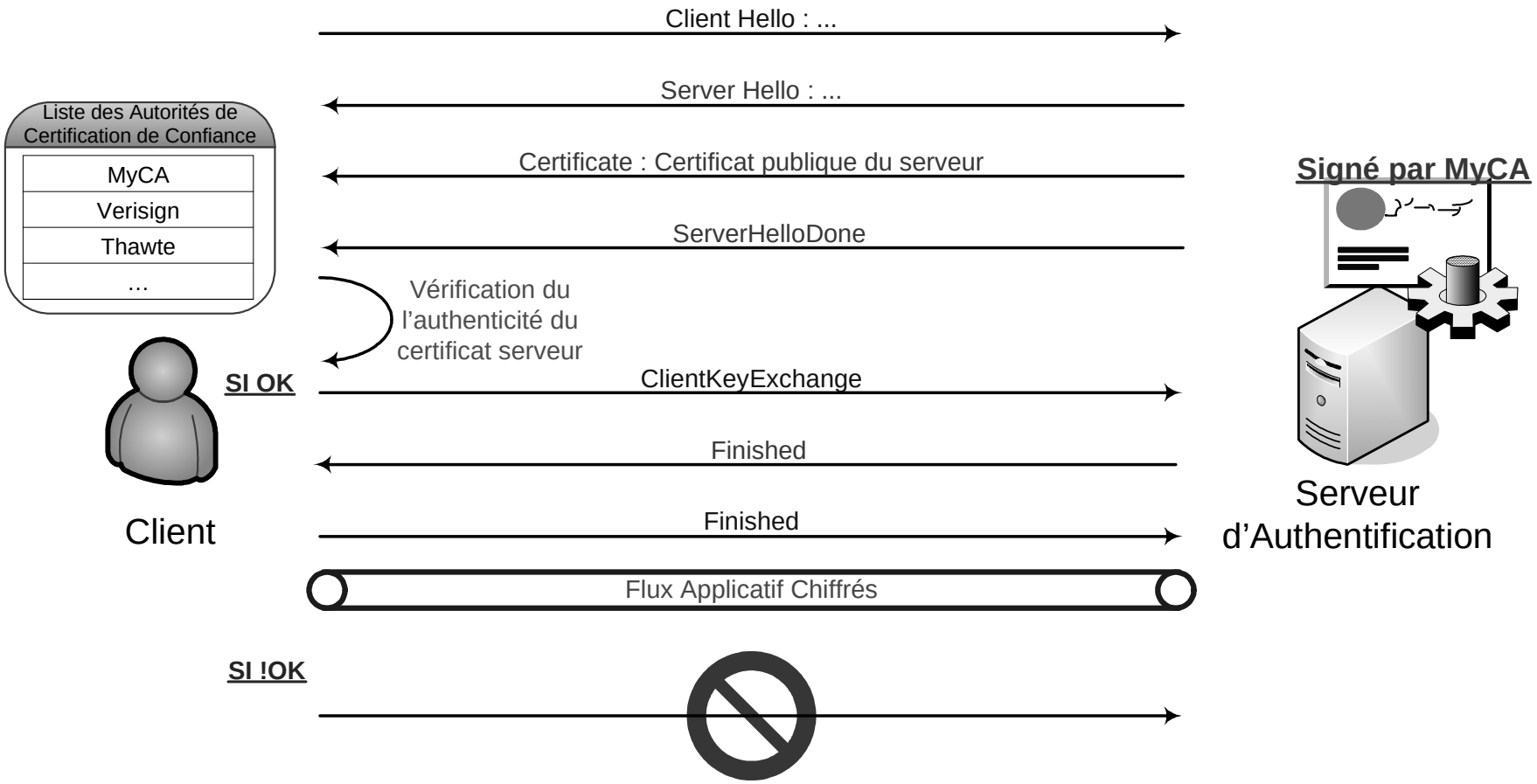
Concepts
Rappels

- VLAN
- DMZ
- Firewall (Statefull, L7)
- Radius

Concepts
Portail Captif



Concepts
TLS



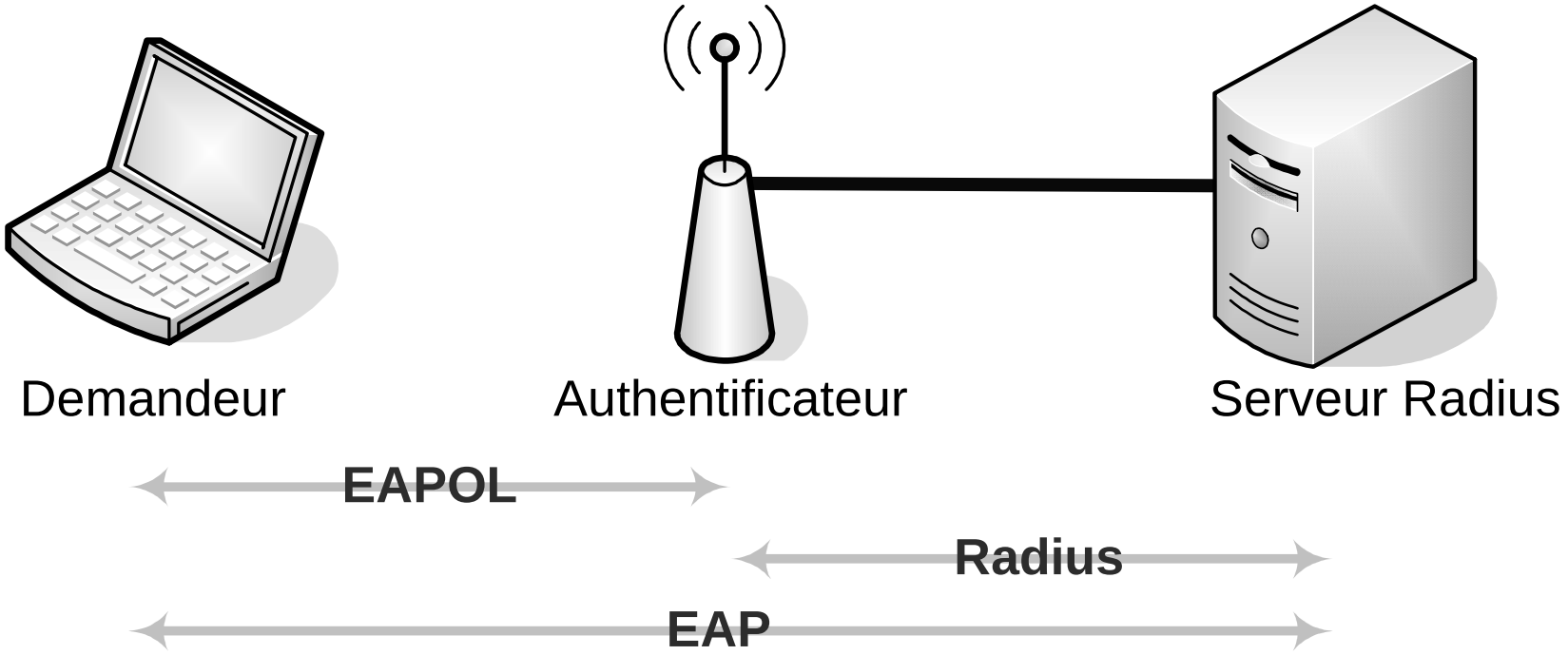
Concepts
802.11i : The security must be set

2 Points majeurs obligatoires :

- Sécurisation de l'accès au média : mécanisme d'authentification (802.1x - EAP)

- Sécurisation du média : mécanismes de chiffrement et de contrôle d'intégrité (AES-CCMP)

Concepts
EAP 1/2



Concepts
EAP 2/2

- Ne pas utiliser les méthodes sans tunnel
  - EAP-MD5
  - EAP-FAST
- Avec tunnel
  - PEAP-MsChapV2
  - EAP-TLS
  - EAP-TTLS

Plan

- Concepts
- **Mise en œuvre**
- Analyse de la sécurité

Mise en Œuvre
Pourquoi du WI-Fi ?

Parce que c'est :

- La classe
- In
- Tendance
- Branché (ou pas)

- Aussi car ça évite les Rogue APs ^_^

Mise en Œuvre
Besoins (ou envies?)

- Accéder aux ressources de l'entreprise :
  - Mail, Intranet, …
  - Partages réseaux : comme à son bureau en tout point
  - Applicatifs : SAP, téléphonie
- Permettre aux invités d'accéder à leurs ressources :
  - Extranet
  - Webmail
  - VPN

Mise en Œuvre
Réponses à ces besoins

2 types d'accès Wi-Fi

- 802.11i pour les « internes »
- HotSpot privé (réseau ouvert) pour les invités
  - Zero Configuration
  - Login/Password unique pour la journée

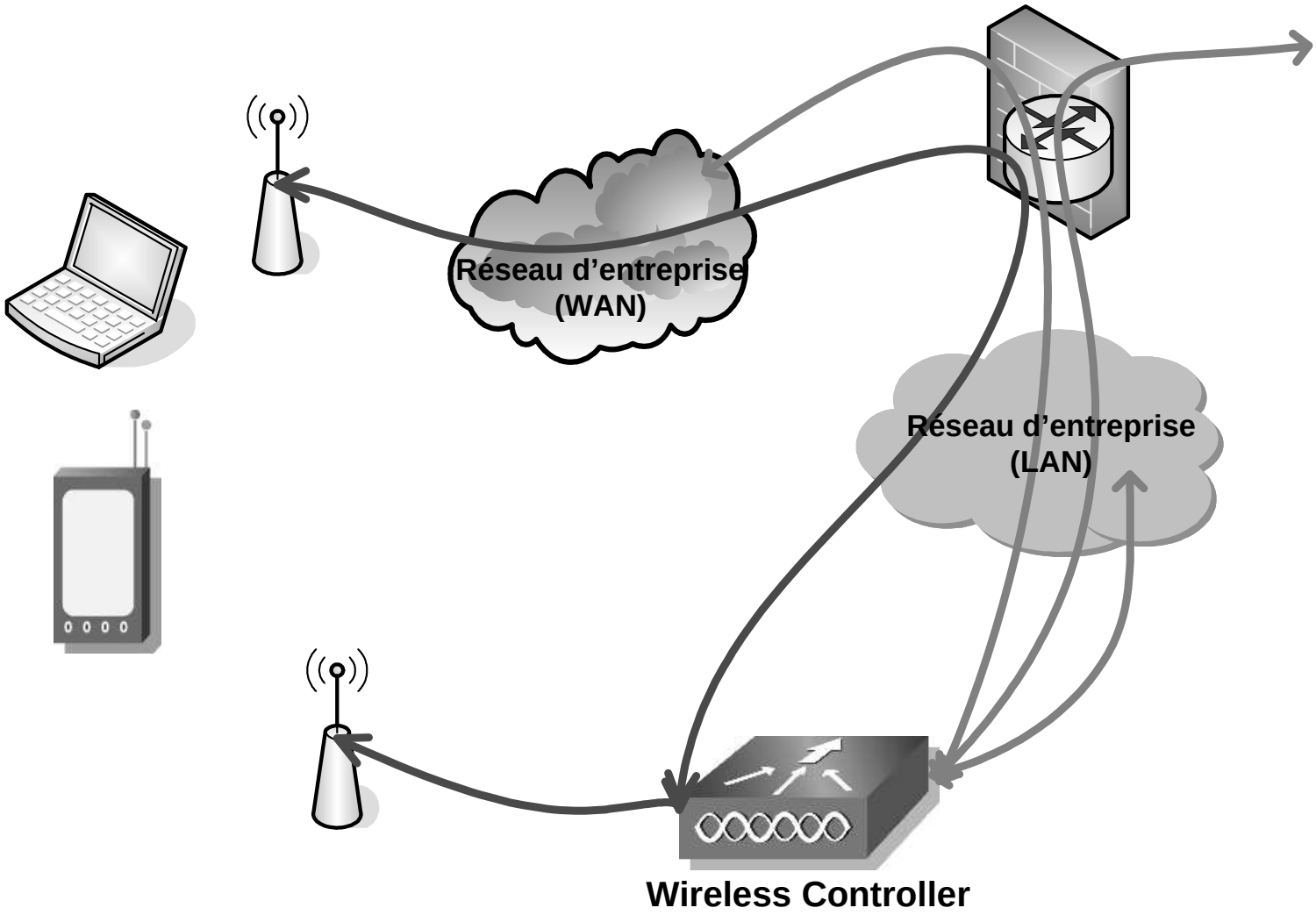
Mise en Œuvre
HotSpot privé

- Réseau en clair, ESSID significatif, page d'accueil avec explication claire
- Configuration des équipements et choix du transit des flux: règles de Firewall ajustées et adaptées, proxy DNS, sortie directe vers proxy Internet, …
- Mise en place de moyens afin de pourvoir identifier l'origine des flux sortants
- Faire prendre conscience aux utilisateurs des dangers des réseaux ouverts : manque d'éducation

Mise en Œuvre
WLAN

- 802.11i est sûr
- Choix importants :
  - méthode d'authentification
  - supplicant
  - serveur AAA / Annuaire
  - Droits / Permissions (accès et flux)

Mise en œuvre
Flux types



Mise en Œuvre
Peurs

- Mon réseau d'entreprise est « visible » (accessible) hors de l'enceinte de mon entreprise.
- Effets sur la santé. Principe de précaution ?

Mise en œuvre
Effets non prévus

- Le niveau de la sécurité mise en œuvre sur le réseau sans fil est très souvent supérieur au réseau filaire existant :
  - Réflexion sur le 802.1x appliqué au LAN
  - Abandon du routage inter-vlan par ACL (ou sans) pour FW
  - …
- Quand ça tombe en panne : c'est la catastrophe ! Les utilisateurs s'habituent très vite aux niveaux services.

Plan

- Concepts
- Mise en œuvre
- **Analyse de la sécurité**

Analyse de la sécurité
Remarques

- Ce n'est pas exhaustif
- Recueil des principales menaces par rapport au média
- Le Wi-Fi n'assure que le transport. Lorsqu'un attaquant à l'accès au média tout est possible, comme un LAN.

Analyse de la sécurité
Vous avez dit « Driver » ?

- Sujet à la mode
  - La saga de l'été dernier
  - Month of Kernel Bugs (nov 06) : 7 PoC en 1 mois

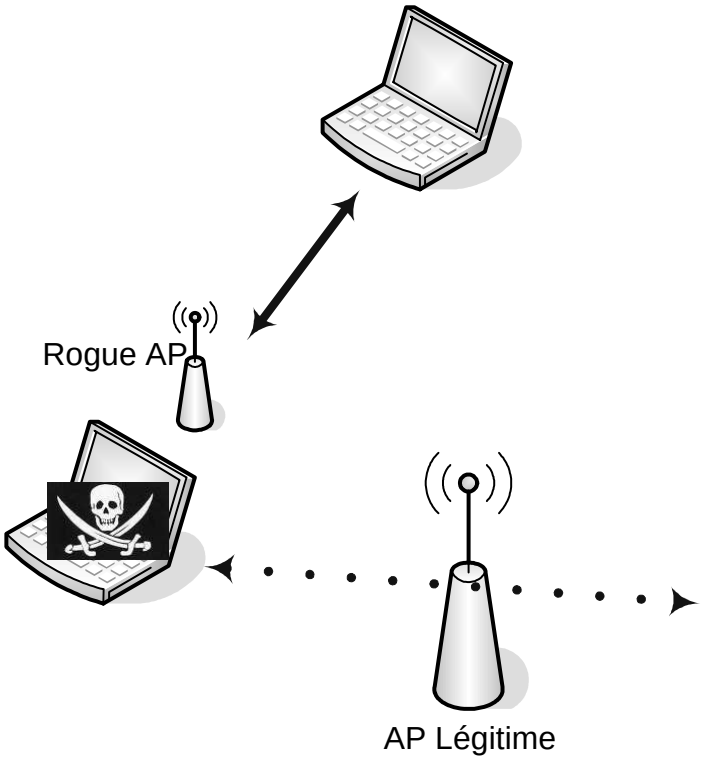
- On peut pas y faire grand chose, à part être « UpToDate »

Analyse de la sécurité
DoS

- DoS « Physique »
  - Le Wi-Fi est avant tout de la radio
    - Brouillage de la bande 2.4GHz et 5GHz
- DoS « Logique »
  - Les trames de management ne sont pas chiffrées, même avec 802.11i : Deauthentication/Disassociation
  - Beaucoup d'autres … (et également sur l'authentificateur!)

Analyse de la sécurité
Rogue AP

- Configurer une borne avec la même configuration : Radio/ESSID/Sécurité
- Multiples possibilités d'actions :
  - Vol de crédits
  - Modification de flux
  - …



Analyse de la sécurité
Reconfiguration

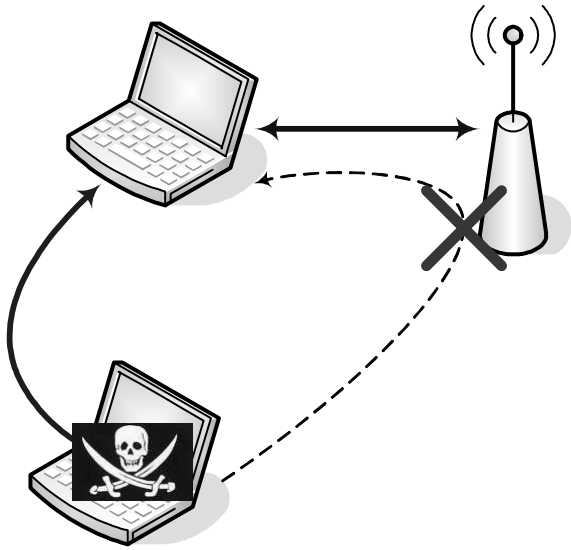
- Attention à l'accès à la configuration des équipements :
  - Changement des mots de passe d'administration
  - Interdire l'administration depuis les interfaces radio
  - Mettre en place des ACL pour la configuration
  - Attention à protéger les sauvegardes de configuration

Analyse de la sécurité
ByPass du portail captif

- Filtrage basé sur :
  - Adresse Mac
  - Adresse IP
  - Adresse Mac + Adresse IP
- Tous ces éléments de filtrage sont usurpables.
- Aucun autre élément unique en commun.

Analyse de la sécurité
Communication directe par injection

- Réseau en clair, se faire passer pour la borne
- Un bit à positionner : « FromDS »
- Permet la communication en direct avec un client associé à un réseau sans fil en clair (fonctionne aussi avec le WEP)
- Aucune parade de cloisonnement possible, directement lié à la norme 802.11



Analyse de la sécurité
TLS MiM

- Donner les droits d'accéder au réseau sans fil uniquement aux personnes qui en ont besoin
- Penser à cocher la case

- La DSI n'est pas forcement maître de tous les dispositifs sans fil utilisés dans l'entreprise
- Utiliser :
  - EAP-TLS (authentification mutuelle par certificats)
  - PEAPv1 ou EAP-TTLS avec des OTP.

Conclusion

- HotSpot privé : si correctement intégré, aucun danger pour l'entreprise qui héberge le service
- WLAN : 802.11i assure une bonne sécurité. Compromis facilité de déploiement/exploitation VS +/- sécurité
- Nécessite une attention toute particulière à la configuration des équipements
- Faire valider l'architecture choisie afin d'identifier les risques résiduels

Questions ?