Wi-Fi en entreprise : Application et Sécurité

Benjamin CHARLES

15 janvier 2008

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
Rappels

- VLAN
- DMZ
- Firewall (Statefull, L7)

Concepts
Fonctionnalités

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

Concepts
Fonctionnalités

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

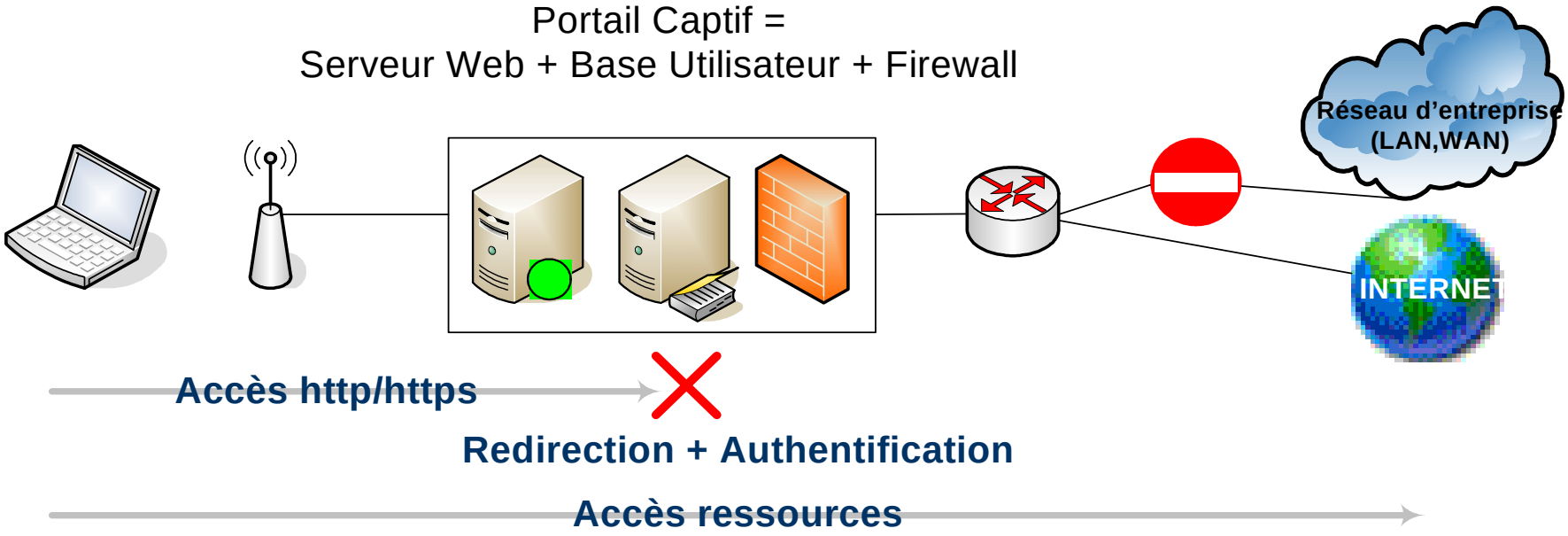
Concepts
Fonctionnalités – Gestion de la radio

- 2 bandes de fréquences :
  - 2,4 GHz : 802.11b (11Mbps) et 802.11g (54Mbps) (13c/!dj)
  - 5 GHz : 802.11a (54Mbps) (19c/dj)
- Attribution automatique du canal, de la puissance selon l'espace RF et la réglementation
- Arrivée de 802.11n (300Mbps)

Concepts
Fonctionnalités

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

Concepts
Fonctionnalités - Portail Captif



Concepts
Fonctionnalités

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

Concepts
Fonctionnalités – AAA

- Authentication , Authorization , Accounting
  - Authentication : Vérifie la validité de l'entité qui se présente
  - Authorization : Valide les services permis à l'entité et exécute les restrictions de l'entité
  - Accounting : Suit l'activité de l'entité

Concepts
Fonctionnalités

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

Concepts
Fonctionnalités – Routeur/Firewall

- Pont L2 = mode extension du LAN
  - ACL
- Routage = mode DMZ Wireless
  - ACL
  - Firewall Statefull
  - Firewall Applicatif

Concepts
Fonctionnalités

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

Concepts
Fonctionnalités – IDS/IPS

- Wireless IDS
  - DoS, Rogue AP, Ad Hoc, Injection de trafic, RF interférences détections
- Wireless IPS
  - Réponse par « containement » des clients ou des APs (DoS vers le client/AP étranger)
- IDS/IPS “classiques” d’analyse du flux

Concepts
Fonctionnalités

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

Concepts
Fonctionnalités – Géo-localisation

- Localiser dans l'espace couvert par l'architecture Wi-Fi (triangulation) :
  - Trouver les utilisateurs (HelpDesk)
  - Localisation des Rogues APs/Clients
  - Localisation des produits/biens
  - Protection des personnes

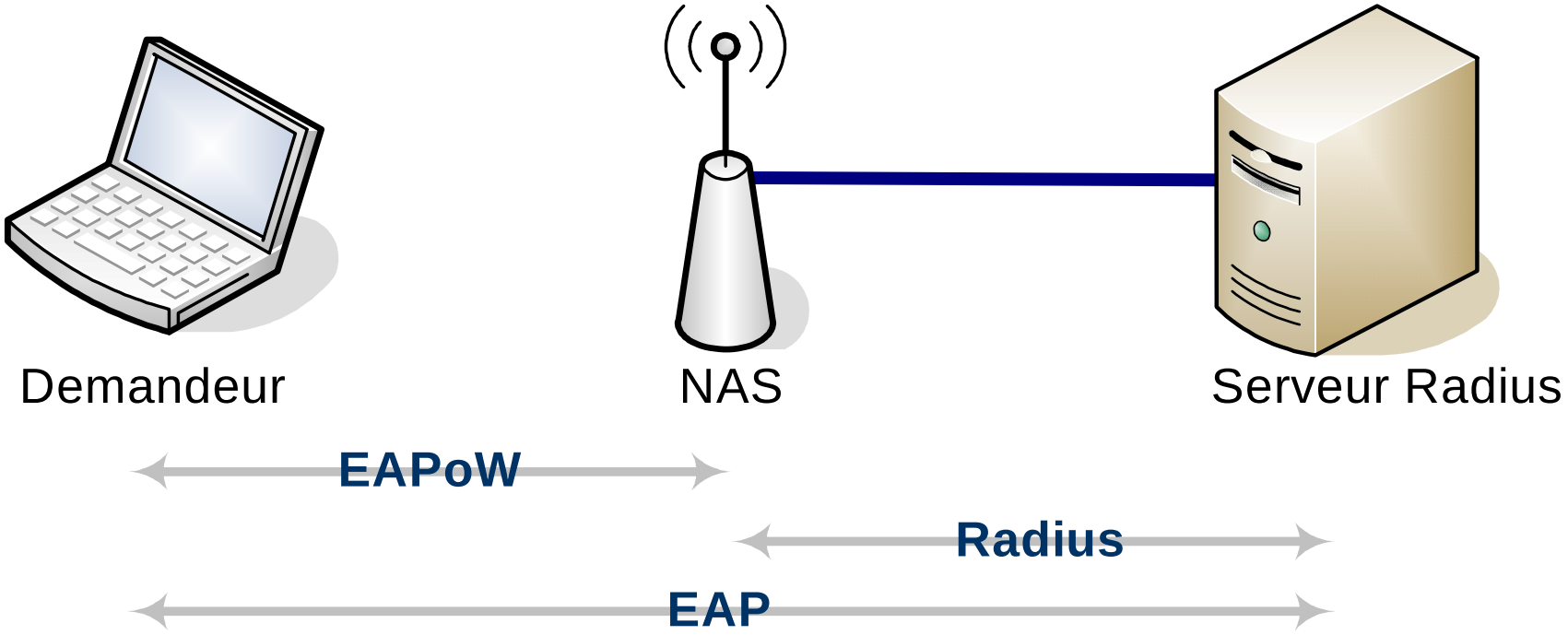
Concepts
802.11i : The security must be set

2 Points majeurs :

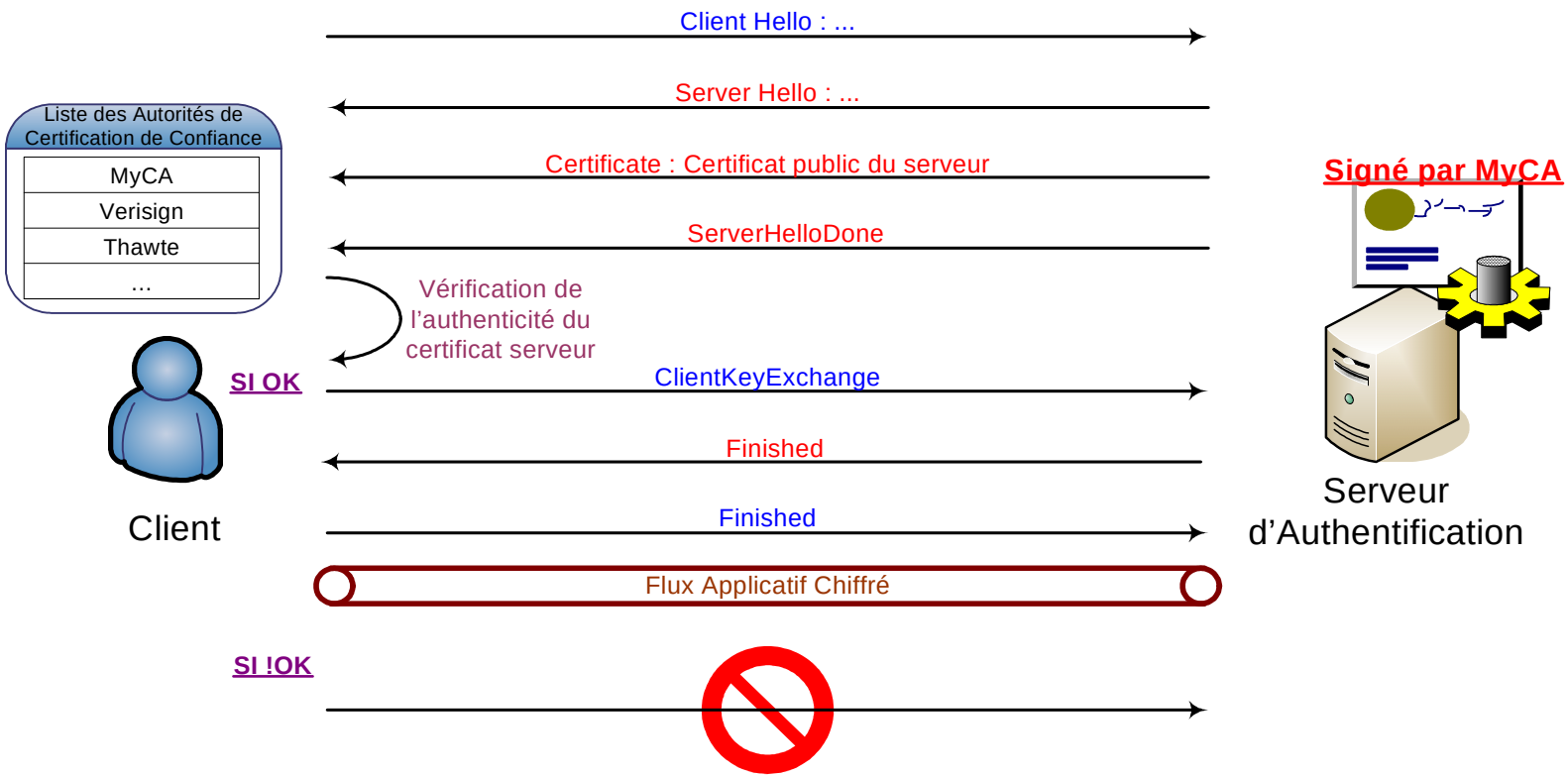
- Sécurisation de l'accès au média : mécanisme d'authentification (802.1x - EAP)

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

Concepts
EAP 1/2



Concepts
TLS



Concepts
EAP 2/2

- Ne pas utiliser les méthodes sans tunnel chiffré :
  - EAP-MD5
  - EAP-LEAP
- Utiliser les méthodes avec tunnel chiffré :
  - EAP-FAST
  - EAP-TLS
  - PEAP
  - 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 Rogues APs ^_^

Mise en Œuvre
Besoins (ou envies ?)

- Accéder aux ressources de l'entreprise :
  - Mail, Intranet, partages réseaux : comme à son bureau en tout point de l'espace couvert
- Permettre aux invités d'accéder à leurs ressources externes :
  - Extranet / Webmail / VPN
- Accéder à des applicatifs spécifiques :
  - SAP, téléphonie sur IP (VoIPoW), …

Mise en Œuvre
Réponses à ces besoins

2 types d'accès Wi-Fi

- 802.11i pour les « internes » (ou s'en rapprochant le plus possible par rapport aux possibilités techniques des terminaux mobiles pour des applications particulières)
- HotSpot privé (réseau ouvert) pour les invités
  - « Zero Configuration »
  - Nom d'utilisateur / Mot de passe unique pour la journée

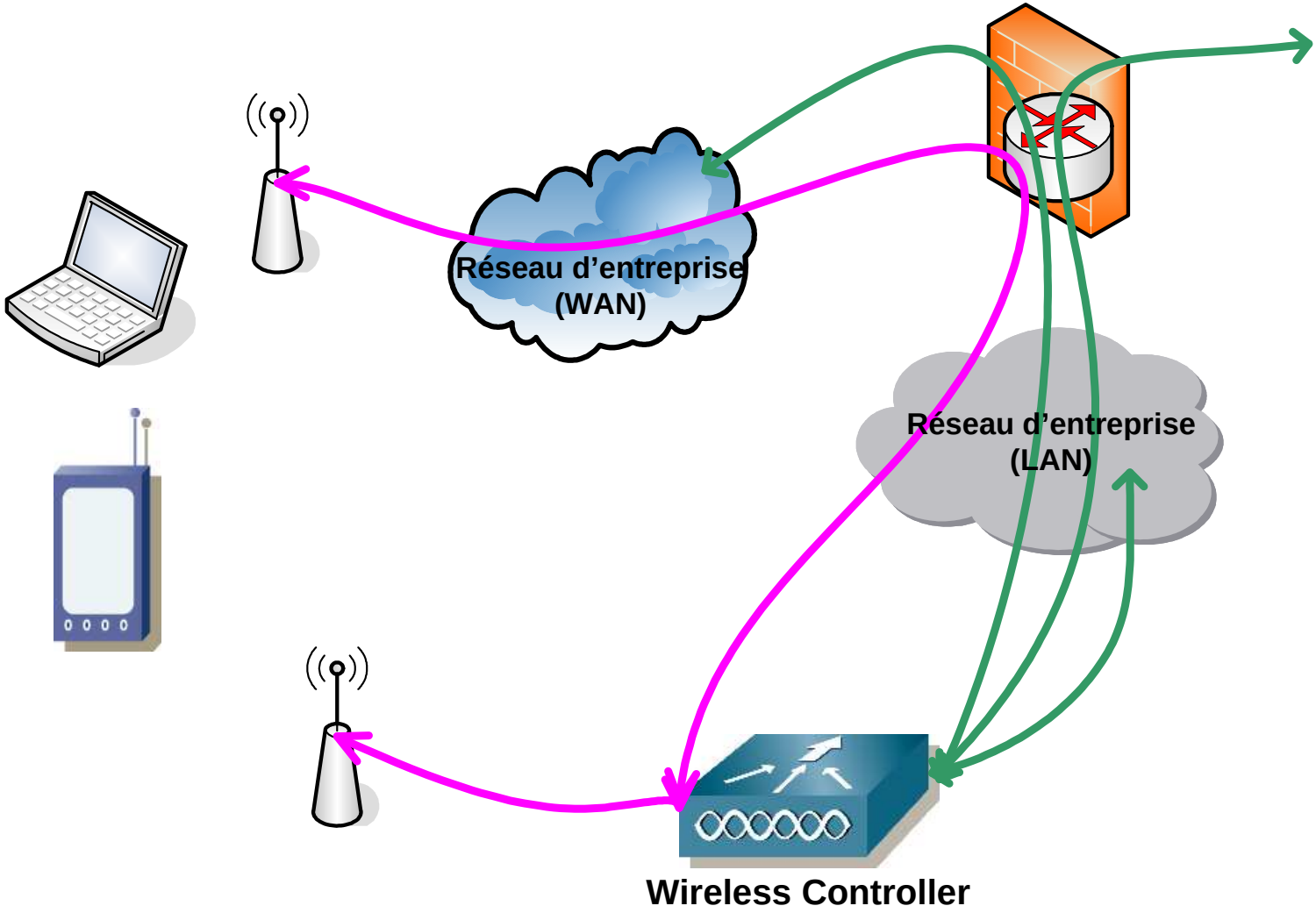
Mise en Œuvre
HotSpot privé

- 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 (LCT)
- 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 (dépend du client et du serveur d'authentification, indépendant de l'infrastructure sans fil)
  - supplicant
  - serveur AAA / Annuaire
  - Droits / Permissions (accès et flux)

Mise en œuvre
Flux types



Mise en Œuvre
Peurs

- Mon réseau d'entreprise est « visible » (donc potentiellement 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 nouveaux 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 accès au média, tout est possible, comme sur un LAN.

Analyse de la sécurité
Vous avez dit « Driver » ?

- Sujet à la mode
  - La saga de l'été 2006
  - Month of Kernel Bugs (nov 06) : 7 PoC en 1 mois

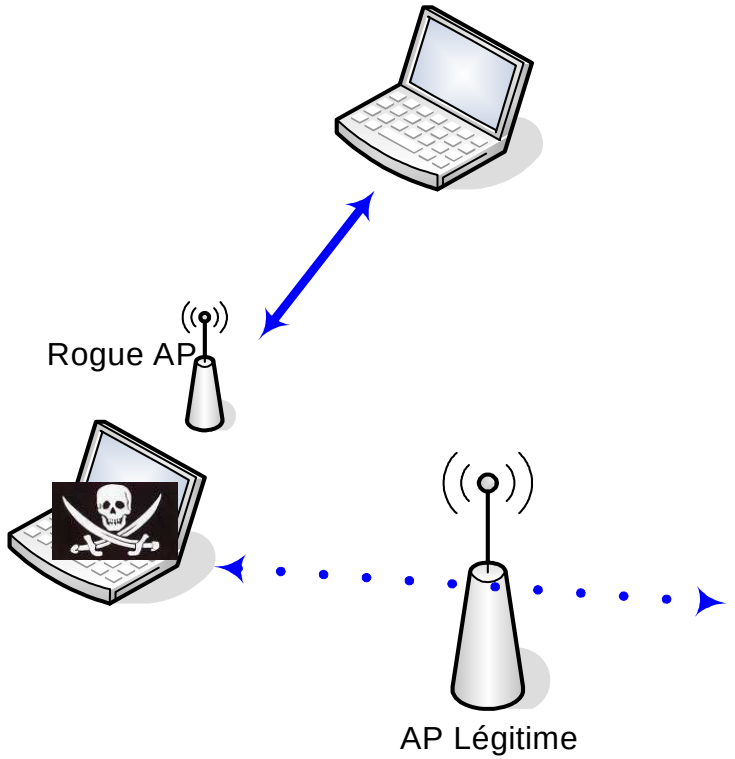
- On ne peut pas y faire grand chose, à part être « UpToDate », du coté client comme du coté architecture

Analyse de la sécurité
DoS

- DoS « Physique »
  - Le Wi-Fi est avant tout de la radio
    - Brouillage de la bande 2.4GHz et/ou 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

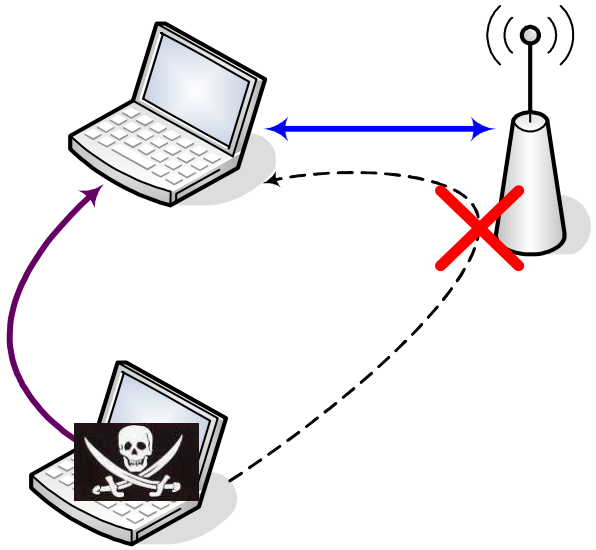
- Attention à l'accès à la configuration des équipements :
  - Changement des mots de passe d'administration
  - Interdire l'administration depuis les interfaces radio
  - Mettre en place des ACLs pour la configuration
  - Attention à protéger les sauvegardes de configuration

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

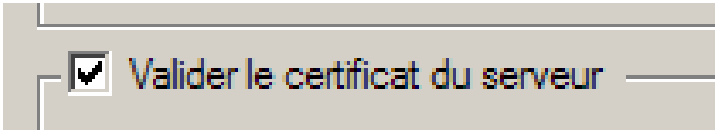
Analyse de la sécurité
Communication directe par injection

- 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 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)
  - PEAP 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 et implémentée afin d'identifier les risques résiduels (audit et test intrusif)

Questions ?