WiFI – Sécurité et nouvelles normes

FRNOG

25 septembre 2003

FRench Network Operators Group

sharing network & security informations

cleclerc@xpconseil.com

Agenda

- **La soupe à l'alphabet et acronymes du 802.11**
  - Normes
  - Les services securité WEP, EAP, TKIP
- **Exploitation et impacts des célèbres vulnérabilités**
  - Les réseaux ouverts (particuliers, entreprises inconscientes).
  - Hotspots - Man in the Middle et Rogue AP
  - DoS
  - WEP
  - EAP/MD5 et LEAP
  - PEAP et EAP/TTLS
- **Les solutions**
  - 802.11i
  - Architecture

l'alphabet et acronymes du 802.11

- **Les Normes**
  - 802.11a/b/g
    - **SSID**

    Le SSID identifie le réseau sans fil
    - **Beacon frame**

    Les Beacon frame servent a annoncer le réseau

    elles ne sont pas diffusées si le réseau est « fermé »
    - **Association Req (Open mode)**

    Ces requêtes sont envoyés par le client après avoir reçu une beacon frame
    - **Probe Req (closed mode)**

    Le client doit connaître le SSID

  - 802.11c/d/e/f
    - **C** spécifie le comportement en mode bridge
    - **D** concerne le comportement des ondes radios
    - **E** spécifie des améliorations concernant la QoS des flux
    - **F** concerne IAPP (Inter Access Point Protocol)

l'alphabet et acronymes du 802.11

- **Les mécanismes de sécurité**

  - **WEP (Wireless Equivalent Privacy)**

    Wep utilise RC4 avec des clés acceptés par le matériel actuel allant de 40 à 256 bits.

    - **Initialisation Vector**

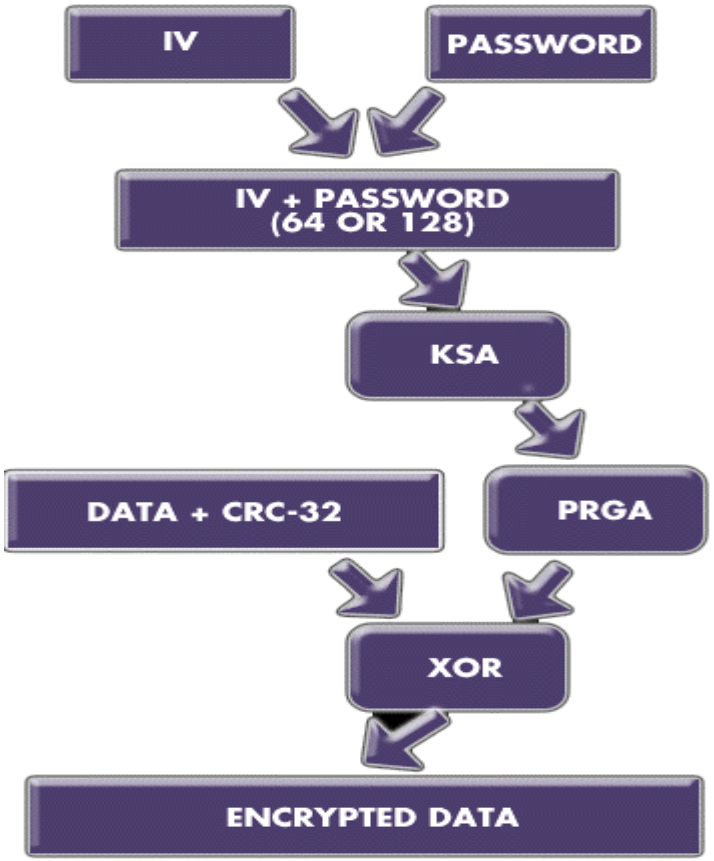
    Il est utilisé afin d'éviter que les mêmes data soit chiffrés de multiple fois avec la même clé.

    - KSA

    Le KSA (Key Scheduling Algorithm) permet de créer un tableau pseudo random à partir de l'IV et de la clé secrete

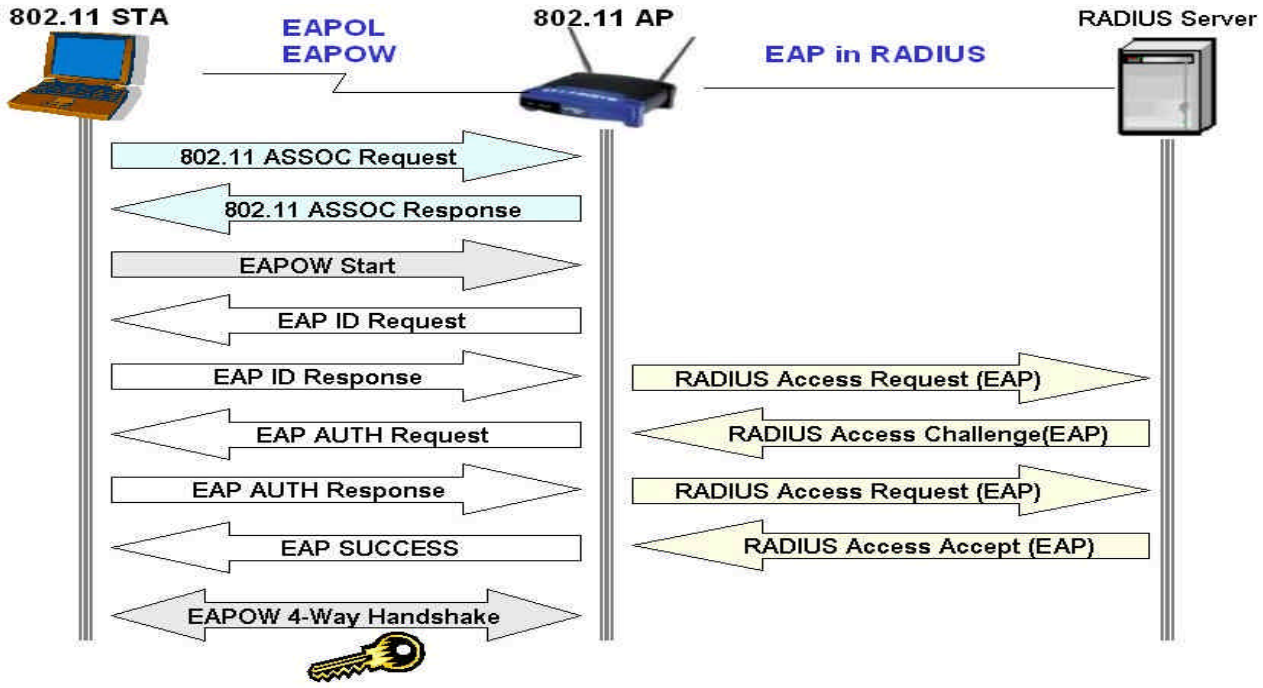
    - PRGA

    Le PRGA (pseudo random generator algorithm) est utilisé pour générer un keystream qui sera XOR avec les données à chiffrer.



l'alphabet et acronymes du 802.11

- **Les mécanismes de sécurité**
  - **EAP (Extensible Authentification Protocol)**
    - Il comporte de nombreuses variantes et permet l'authentification du client



l'alphabet et acronymes du 802.11

- Types EAP

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Authentification du serveur	Aucune	Password Hash	Clé publique (certificat)	Clé publique (certificat)	Clé publique (certificat)
Authentification du client	Password Hash	Password Hash	Clé publique (Certificat , carte à puce)	CHAP, PAP, MS-CHAP(v2), EAP	EAP(EAP-MS-CHAPv2 ou clé publique)
Distribution dynamique des clés	Non	Oui	Oui	Oui	Oui
Risques sécurité	Vol de session. Attaque dictionnaire. Obtention du login client et Attaque MiM	Attaque dictionnaire et obtention du login client	Obtention de l'identité client	Attaque MiM	Attaque MiM

l'alphabet et acronymes du 802.11

- **802.1x**
  - 802.1x permet d'utiliser EAP sur les liaisons Ethernet et ici 802.11
- **TKIP (Temporal Key Integrity Protocol)**
  - TKIP utilise toujours RC4 (et donc ses faiblesses)
  - Le filtrage des IVs faibles est standard
  - La clé est renouvelée tout les 10000 paquets
- **WPA**
  - Wi-Fi protected Access
  - Les produits actuels peuvent être mis à jour pour être conforme WPA
  - Pour être WPA le produit doit implémenter 802.1x et TKIP.
  - Pas de protection des associations
  - Pas d'AES

Exploitation et impacts des célèbres vulnérabilités

- **Les réseaux ouverts (hotspots, particuliers, entreprises inconscientes)**
  - **Netstumbler**
    - Découverte des réseaux Wi-Fi sous windows
    - Couplé avec un GPS, il est possible de réaliser des cartes.
  - **Kismet**
    - Equivalent texte (*nix & win32).
  - **Ethereal, tcpdump**
    - Une fois la libpcap à jour, ils peuvent écouter le 802.11
  - **Airjack**
    - Permet l'injection de paquets 802.11

Exploitation et impacts des célèbres vulnérabilités

- **Les hotspots**
  - **Les risques :**
    - Authentification souvent http
    - Ecoutes entre utilisateurs
    - Man in the middle (arpspoof)
    - Airsnarf permet d'activer un faux AP avec une fausse mire de login en quelques minutes
  - Les operateurs Wireless doivent modifier leurs pratiques :
    - Mécanismes d'authentification forte, interdiction des authentifications simultanées, surveillance de l'existance et de la création d'AP , chiffrement des données utilisateur,etc …

Exploitation et impacts des célèbres vulnérabilités

- **Les DoS**
  - **Emission de fréquences parasites**
    De nombreux matériels peuvent être utilisés… (Micro-onde, camera wireless,…)
  - **Rogue AP**
    Par défaut les clients Wi-Fi s'associent sur l'AP qui émet le plus fort.
  - **Airjack**
    Forger des trames de désauthentification,désassociations.
  - **Attaques contre EAP**

Exploitation et impacts des célèbres vulnérabilités

- **Le WEP**

  On peut aujourd'hui casser du WEP avec quelques clics sous linux et quelques commandes sous BSD. La problématique est la durée de capture et le trafic nécessaire.

  Les faiblesses du WEP sont multiples, la plus importantes est la diffusion des IVs en clair dans les paquets et des faiblesses dans leur génération.

  - **Airsnort**
    - Il faut environ 6 millions de paquet pour retrouver la clé.
  - **Bsd Air Tools** (dashb0den)
    - Un « ping –f –s 1 » de 30 minutes suffit pour retrouver la clé.
  - **WepWedgie et Wnet**
    - Ces deux outils (un linux et l'autre openbsd3.2) permettent de réinjecter du faux trafic afin que les réponses légitimes servent à alimenter l'outil de capture.

Exploitation et impacts des célèbres vulnérabilités

EAP/MD5 et LEAP

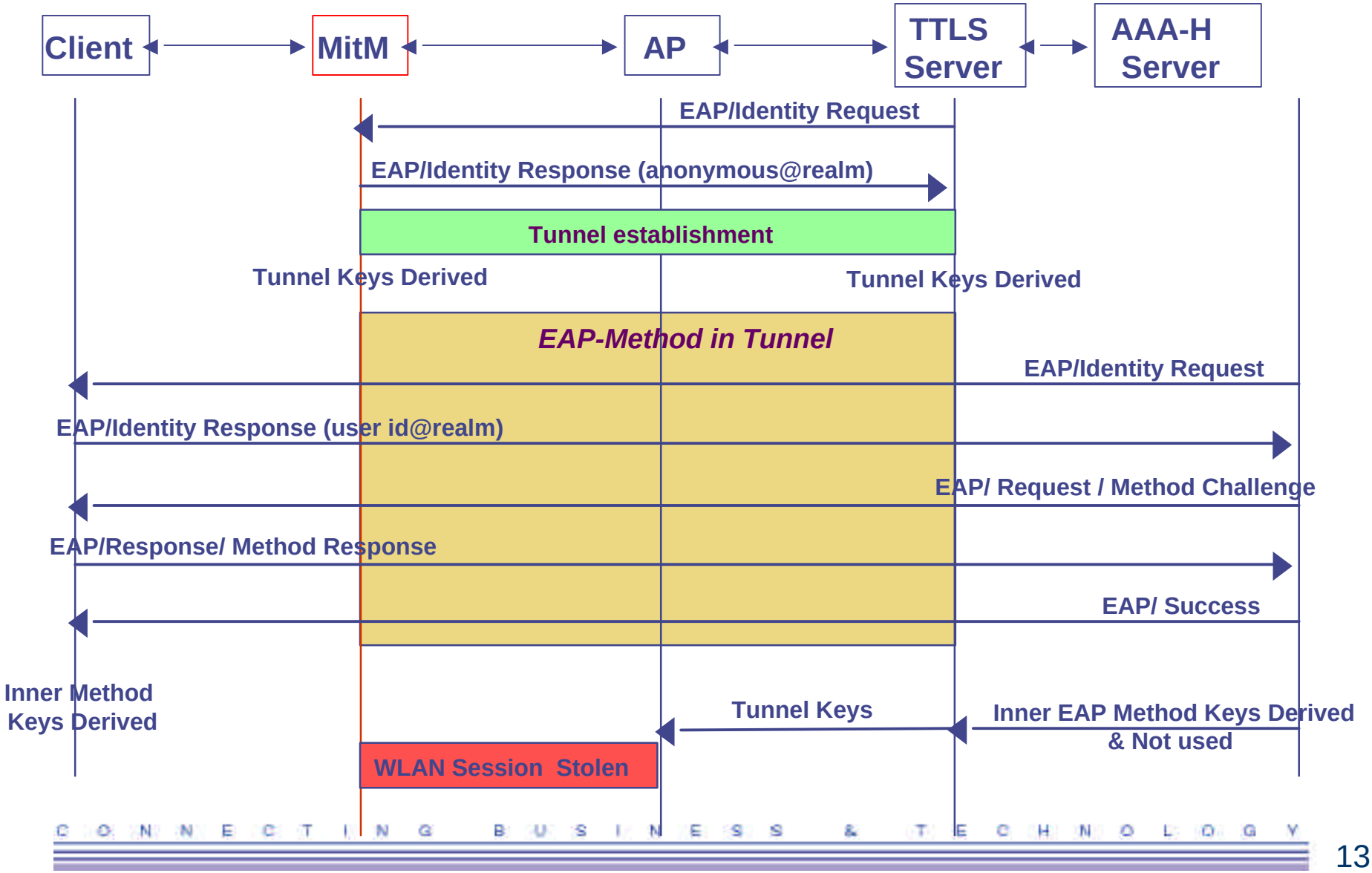
- Ces deux protocoles laisse circuler l'identifiant en clair et le mot de passe peut être cassé hors ligne.

- Ethereal, tcpdump
  - Il suffit de lire les trames pour identifier le login de l'utilisateur.
- Anwrap
  - Permet le bruteforcing de l'authentification LEAP

PEAP/TTLS

- Il n'y a pas d'outils diffusés actuellement.
- Cependant des attaques MiM sont possibles.

Man in the Middle pendant une authentification EAP/TTLS

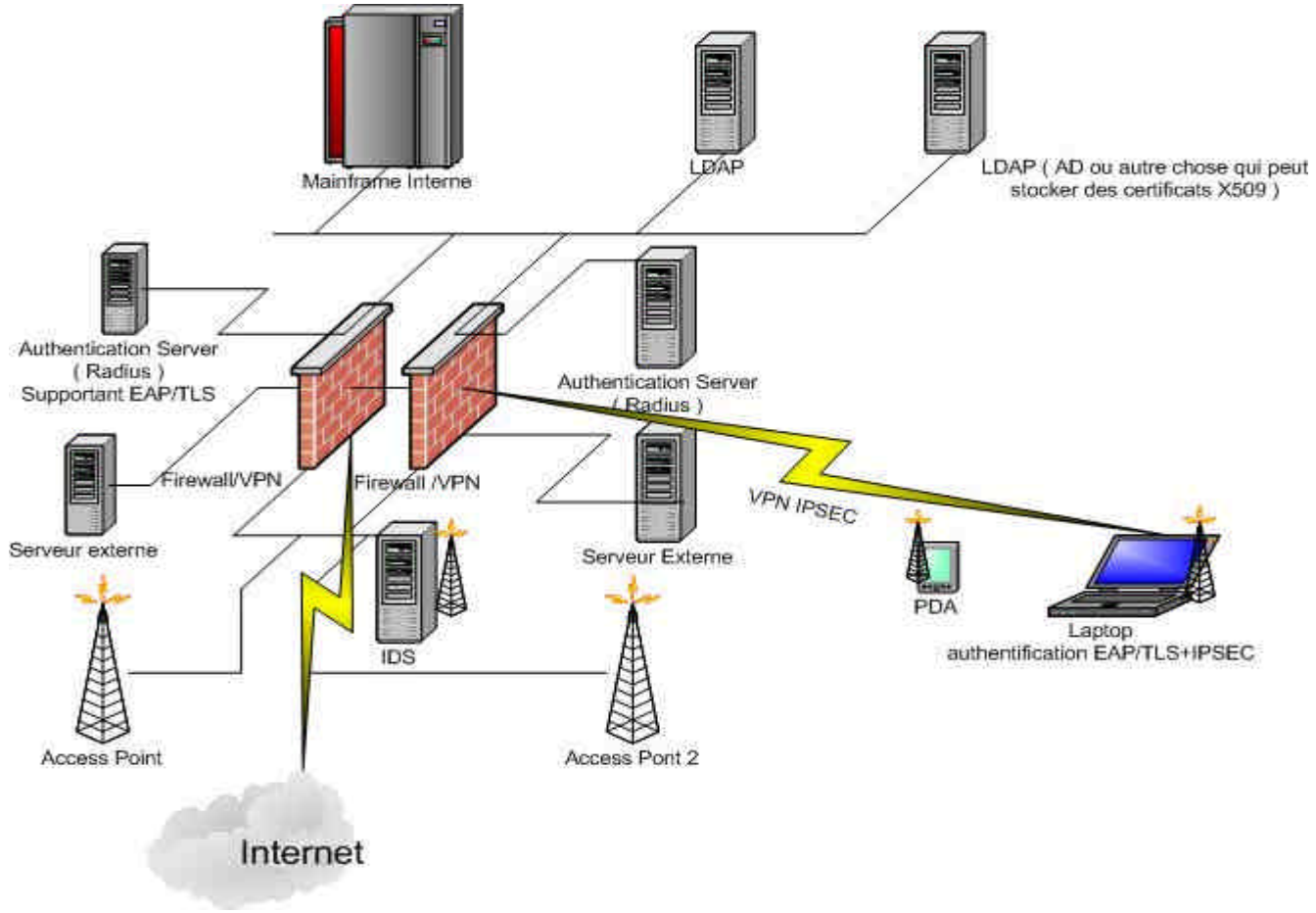


Les solutions

- **802.11i**
  - Apports de 802.11i :
    - AES
    - EAP Obligatoire
    - Sécurisation des fonction de management (associations, désassociations)
    - Nécessite un renouvellement du matériel.

Les solutions

Architecture



Conclusion

- **Beaucoup de problèmes**
- **Beaucoup de protocoles et de solutions**
- **Laquelle choisir ?**