Réseaux sans fils et mobiles

Pr M. EL HALOUI

Rappels

- Couche physique : méthodes d'accès et protocoles
- FHSS, DSSS, IR, CCK
- Modulation/ Démodulation (FSK, ASK, PSK)
- Multiplexage (FDM, TDM, CDM)
- Couche liaison : composition et mécanismes
- CSMA, CSMA/CD, CSMA/CA
- Questions ?

Sécurité : Défis pour les réseaux WIFI

- Problématiques :
  - le support de transmission est l'air.
  - les ondes radio étant un support de transmission partagé
  - quiconque se trouvant dans la zone de couverture peut écouter le support et s'introduire dans le réseau
  - En plus, un réseau Wi-Fi doit se protéger des attaques classiques

- Ces failles de sécurité ont porté atteinte au développement du WIFI en entreprise,
- Il existe des moyens de sécurité implantés de base sur le matériel Wi-Fi (carte et point d'accès)
- D’autres mesures de sécurité sont nécessaires

Sécurité : Type d’attaques

- Attaques Passives : recherche de points d'accès à l’aide de solutions scanners. Les sites détectés sont ensuite indiqués par un marquage (Open, Closed, WEP node). Ensuite déchiffrer les clés WEP avec des logiciels spécifiques.

- Attaques Actives :
  - **Les dénis de services** : Consiste à empêcher des utilisateurs légitimes d'accéder à des services en saturant de fausses requêtes ces services (Ex. Inonder l’AP par des requête d’authentification)
  - **Spoofing (usurpation d'identité) :** technique permettant à un pirate d'envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate.
  - **Man in the middle (home au milieu)** : disposer un point d'accès étranger dans à proximité des autres PA légitimes. Les stations livreront au « Faux PA » leurs informations nécessaires à la connexion.
  - **Brouillage radio :** Création de système radio générant du bruit dans la bande des 2,4 GHz.

Sécurité : Type d’attaques

- Autres Types d’attaque :
  - **Craquage de mots de passe :** Consiste à faire beaucoup d'essais pour déterminer un mot de passe. Soit par utilisation de dictionnaires ou par essai de toutes les combinaisons possibles.
  - **Backdoors :** ou porte de derrière, crée par un pirate une fois qu’il arrive à accéder à un système. Le but est de faciliter l’accès par la suite (Ajout de compte Admin, modification de règles de filtrage,…)
  - **Le sniffing :** attaque est basé sur l'interception de données émises sans précaution à toutes les parties comme lors des diffusions

Sécurité : Sévices de sécurité

- **Chiffrement (la cryptographie) :** consiste à **rendre un texte incompréhensible en le codant** à l'aide d'une clé de chiffrement. Le destinataire déchiffre le texte codé à l'aide d'une clé de déchiffrement. Il existe trois méthodes :
  - ***clé symétrique*** : clé de chiffrement identique à la clé de déchiffrement. Exemple d'algorithmes : DES (Data Encryptions Standard), IDEA (International Data Encryptions Algorithm), RC (Ron's Code), AES (Advanced Encryption Standard)
  - ***clé asymétrique*** : Une clé privée et une clé publique. Exemple d'algorithmes : RSA (Rivest, Shamir, Adelman).
  - ***clé mixte*** : utilisation des deux précédentes. Exemple PGP (Pretty Good Privacy)
- **Certificats :** permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. délivré par un organisme appelé autorité de certification (CA : Certification Authority). Géré par le standard X509 de l'UIT.

Sécurité : Sévices de sécurité

- **Authentification :** garantir l'identité des correspondantes. Le mode le plus simple est l'utilisation d'un identificateur et d'un mot de passe. Exemple de protocoles : Tacas+ (CISCO), Kerberos (Origine UNIX, adopté par Microsoft),…
- **Intégrité des données** : Assurer simplement que les données sont intégrés, c'est-à-dire qu'elles n'ont pas été au passage falsifiées par un intrus.
- **Non répudiation** : signifie la possibilité de vérifier que l'émetteur et le récepteur sont bien les parties qui ont respectivement envoyé ou reçu un message
- **Contrôle d'accès** : Mise en place des moyens de contrôle d'accès et une architecture réseau sécurisée (firewall,….).

Sécurité WIFI : protections de base

Les protections de base pour un réseau WIFI :

- Sécuriser le point d’accès (AP)
- Agir sur l'identifiant du réseau (SSID)
- Filtrage d’adresse MAC
- Utiliser la une Clé WEP (64, 128 ou 256 bits)

Sécurité WIFI : Sécuriser le point d'accès (AP) :

- Bien choisir l'emplacement (Eviter les murs extérieurs)
- Réglage de la puissance d'émission des bornes (Adapter aux cellules à couvrir)
- Eviter les valeurs par défaut (Login et PWD admin lors de l'installation)
- l'identifiant du réseau SSID :
  - changement de SSID par défaut (voire une modification régulière,…)
  - désactivation de la diffusion (Broadcast) du SSID
- Désactivation des services d'administration disponibles (DHCP, Interface Web, SNMP, TFTP,…)
- Mettre à jour le firmware des bornes et des cartes

Sécurité WIFI : Filtrage d'adresse MAC

- utilisation des ACL (Access List) au niveau du AP qui permet le filtrage des @MAC des équipements autorisés.
  - Renseigner les @ MAC autorisées en local sur chaque point d'accès.
  - En utilisant un serveur Radius (serveur d'authentification pour centraliser les @ MAC autorisées).
- Attention : certains adaptateurs permettent de modifier leurs adresses MAC
- Administration difficile en local surtout si le nombre de clients et de points d'accès sont importants.
- Même en serveur centralisé, toutes les @MAC en clair dans le fichier de configuration radius.

Sécurité WIFI : Utilisation de Clé WEP

- WEP (Wired Equivalent Privacy) : Confidentialité équivalente au réseau filaire
- Période : 1999 à 2004
- Objectif : Offrir une solution de cryptage des données.
- Principe : Chiffre le corps de la trame MAC et le CRC avec RC4 (algorithme de cryptage) en utilisant des clefs de 64, 128 ou 256 bits (dont 24 bits réservés à l'initialisation c.à.d. 40 bits pour le chiffrement pour une clé de 64 bits)
- Le chiffrement n'est utilisé qu'entre les éléments 802.11. Il ne s'applique plus sur le réseau filaire.

Sécurité WIFI : Utilisation de Clé WEP

- Limites et faiblesses :
  - Clés statiques partagées
  - Rarement changées
  - Vol de machine donc vol de clef
  - Les autres qui partagent la clef peuvent lire vos trames
  - Possède une durée de vie longue
  - Diffusion d'une nouvelle clé difficile si le parc de mobile est important.
  - Peu être cassée (combinaisons de caractères imprimables)

Sécurité WIFI : Utilisation de Clé WPA

WPA (Wi-Fi Protected Access) :

- Crée en 2003, pour combler les faiblesses de WEP
- Protocole développé par l'IEEE pour la sécurisation des réseaux sans fil
- Assure au niveau de la couche 2 les fonctions de **cryptage** et **intégrité des données** ainsi que l'**authentification** des stations mobiles.
- Permet une sécurité en utilisant des clés **TKIP** (**T**emporal **K**ey Integrity **P**rotocol) dites dynamiques
- Utiliser une clé par station connectée à un réseau sans fil (au lieu d'une clé partagée dans le WEP)
- Les clés WPA sont générées et distribuées de façon automatique par le point d'accès
- Lors de la transmission de chaque trame une vérification de l'intégrité des informations est réalisée

Sécurité WIFI : Utilisation de Clé WPA

WPA (Wi-Fi Protected Access) :

- Existe en deux modes :
  - **WPA Personal** ou WPA PSK (Pre-Shared Key) :
    - Destiné aux réseaux personnels ou de petites entreprises, car ne nécessite pas un serveur d'authentification.
    - utilisation d'une clé partagée, appelées PSK pour Pré-Shared Key, renseignée dans le point d'accès ainsi que dans les postes clients
    - Demande la saisie d'une phrase secrète, traduite en PSK par un algorithme de hachage
  - **WPA Enterprise** (norme 802.1x), basé des rôles :
    - **Le client (***Supplicant***)**, la station qui veut se connecter
    - **Le contrôleur (***Authenticator***)**, un périphérique qui contrôle l'accès (Point d'accès)
    - **Le serveur d'authentification (***Authentication server),* en général un serveur RADIUS (Remote Authentication Dial-In User Service) qui détermine les services auxquels le demandeur a accès
    - **Un annuaire** de données utilisateurs (LDAP)

Sécurité WIFI : Utilisation de Clé WPA2/ WPA3/ EAP

WPA 2 (IEEE 802.11i) :

- Successeur ratifié de WPA en 2004
- Reprise de la grande majorité des principes et protocoles apportés par WPA
- Intégration de l'algorithme de chiffrement AES (Advanced Encryption Standard)
- Adoption de nouvelles méthodes de chiffrement s'appuyant sur l'AES (CCMP, WRAP,…)

WPA 3 (IEEE 802.11s)

- Validé en 2018
- Remplace la clé partagé PSK (**P**ré-**S**hared **K**ey) par SAE (Simultaneous Authentication of Equals) qui permet de s'échanger des clés sans les exposer au moment de l'échange.
- Chiffrement renforcé par le protocole GCMP (Galois/Counter Mode Protocol) basée sur l'algorithme AES.

EAP (Extensible Authentification Protocol) :

- Fait partie du standard standard 802.1x.
- Un protocole qui se base sur puiseurs méthodes d'authentification (Kerberos, mot de passe jetable, SIM, Carte à puce,….)