Sécurité des Systèmes Informatiques

Houssem MAHMOUDI houssem.mahmoudi@ensicaen.fr

AU : 2024-2025

L'École des INGÉNIEURS Scientifiques

CHAPITRE 4 : SÉCURITÉ DE RÉSEAUX WIFI

Introduction au réseau Wifi

I. Introduction au réseau Wifi

1. Présentation

- Le réseau WiFi (Wireless Fidelity) est une technologie de communication sans fil permettant la transmission de données sur un réseau informatique en utilisant des ondes radioélectrique.
- Il repose sur les normes IEEE 802.11, définies par l'Institute of Electrical and Electronics Engineers (IEEE)

I. Introduction au réseau Wifi

2. La Norme 802.11 et ses extensions

Normes	Définition
802.11	1ère norme en 1997, débit limité à 2Mbps
802.11a	1999, Bande de fréquence 5GHz, débit 54 Mbps
802.11b	1999, Bande de fréquence 2.4GHz, débit 11 Mbps
802.11g	2003, Bande de fréquence 2.4GHz, débit 20~25 Mbps (Extension de 802.11b)
802.11n	2009, offre un débit de 600 Mbps
802.11ac	2013, Wifi 5, Bande de fréquence 5GHz, offre un débit de 1 Gbps
802.11ax	2019, Wifi 6, Bande de fréquence 2.4/5 GHz, offre un débit de 1~2 Gbps
802.11be	2024, Wifi 7, Bande de fréquence 2.4/5/6 GHz, offre un débit de 5~10 Gbps

I. Introduction au réseau Wifi

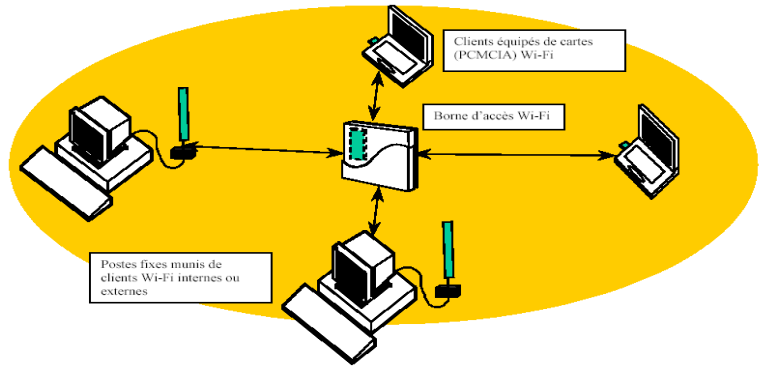
3. Avantages & inconvénients

Avantages	inconvénients
• Mobilité	• Sécurité vulnérable
• Installation facile	• Interférences
• Accessibilité	• Débit faible sur les longues distances.
• Coût réduit	• Consommation d'énergie plus que le filaire
• Flexibilité	• Latence par rapport à Ethernet

I. Introduction au réseau Wifi

4. Mode Infrastructure

- Le Mode Infrastructure est une configuration de réseau sans fil où les appareils communiquent via un point d'accès central



I. Introduction au réseau Wifi

5. Mode Ad hoc

- Dans ce mode, les appareils peuvent communiquer directement entre eux sans passer par un point d'accès.

Réglementations du réseau Wifi

II. Réglementation du réseau Wifi

1. Aspects légaux

- L'utilisation des réseaux WiFi est soumise à des réglementations spécifiques qui varient selon les pays.
- Ces réglementations concernent :
  - La bande de fréquences utilisées
  - La puissance de l'émission
  - Protection des données

II. Réglementation du réseau Wifi

2. Réglementation des fréquences

- Le WiFi utilise des bandes de fréquences définies par les autorités de régulation de chaque pays.
- Les principales autorités sont :
  - **FCC** (Federal Communications Commission - USA)
  - **ETSI** (European Telecommunications Standards Institute - Europe)
  - **ARCEP** (Autorité de régulation des communications électroniques - France)
- En Europe, certaines sous-bandes de 5 GHz nécessitent une limitation de puissance pour éviter les interférences avec certains matériels (Radar,…)

II. Réglementation du réseau Wifi

3. Aspects juridiques

- L'utilisation non réglementée du WiFi peut entraîner des amendes et sanctions :
  - Amendes en cas de dépassement des limites de puissance ou d'utilisation illégale d'une bande de fréquence.
  - Poursuites judiciaires si un réseau est utilisé pour des activités illégales (piratage, diffusion de contenus interdits…).
  - Fermeture d'un réseau WiFi public non conforme.

Menaces et vulnérabilités des réseaux WiFi

III. Menaces et les attaques sur le réseau WiFi

1. Absences de chiffrement

- Sans chiffrement, les données circulant sur le réseau Wifi peuvent être interceptées par des attaquants à l'aide de simples outils comme Wireshark ou Aircrack-ng.
- Risques :
  - Vol des données sensibles
  - Usurpation d'identité
  - Injection des malwares

III. Menaces et vulnérabilités des réseaux WiFi

2. Sniffing

- Le sniffing : consiste à écouter les transmissions des différents utilisateurs du réseau sans fil. (Wardriving est illégal).
- **Wardriving** : Action pratiquée par des groupes de passionnés par la radio, se promener en voiture avec une antenne WiFi pour détecter et cartographier les réseaux Wifi vulnérables et les exploiter

III. Menaces et vulnérabilités des réseaux WiFi

2. Sniffing – Wardriving

III. Menaces et vulnérabilités des réseaux WiFi

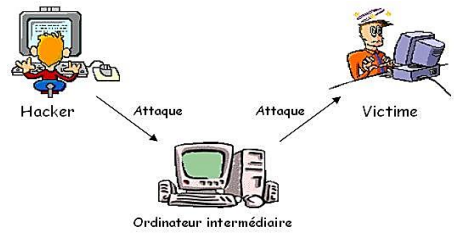
3. Rogue Access Point

- Un Rogue Access Point est un faux point d'accès WiFi installé par un attaquant pour tromper les utilisateurs et capturer leurs données.
- Méthode d'attaque :
  - L'attaquant crée un point d'accès WiFi avec un nom similaire à un réseau existant (exemple : "FreeWifi_secure" au lieu de "FreeWifi").
  - Les utilisateurs s'y connectent sans méfiance.
  - L'attaquant intercepte les données transmises (mots de passe, emails, requêtes web).

III. Menaces et les attaques sur le réseau WiFi

4. Attaque Man in the Middle

- L'attaque MITM (Homme du Milieu) consiste à intercepter, modifier et relayer les communications entre un utilisateur et un serveur.
- L'attaquant peut alors espionner les échanges ou injecter du contenu malveillant.



III. Menaces et les attaques sur le réseau WiFi

5. Déni de service

- Une attaque DoS (Denial of Service) vise à rendre un réseau WiFi inutilisable en inondant le point d'accès par de requêtes ou en exploitant des vulnérabilités du protocole WiFi.
- Techniques :
  - Jamming WiFi : Brouillage du signal avec des ondes parasites
  - Désauthentification (Deauthentication Attack) : Envoi de faux paquets de désauthentification pour forcer les utilisateurs à se reconnecter.
  - Flooding (inondation de requêtes) : Envoi massif de requêtes pour saturer le point d'accès.

III. Menaces et les attaques sur le réseau WiFi

6. Attaque Evil Twin

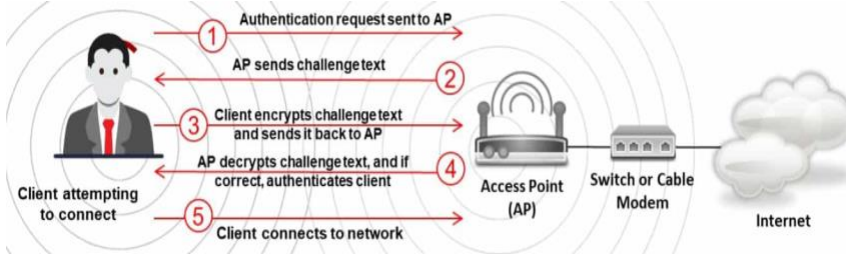
- L'attaque Evil Twin est une version plus sophistiquée du Rogue Access Point.
- L'attaquant duplique un réseau WiFi légitime avec les mêmes paramètres (SSID, type de chiffrement,…) pour piéger les utilisateurs.
- Les scénarios de l'attaque Evil twin sont :
  - Capture de trafic non chiffré (HTTP, DNS,…)
  - Attaque SSL Strip (Downgrade HTTPS vers HTTP).
  - Attaque Man-in-the-Middle (MITM) sur HTTPS : installer faux certificat SSL sur la machine victime.

Processus d'authentification dans les réseaux Wifi

IV. Processus d'authentification dans les réseaux WiFi

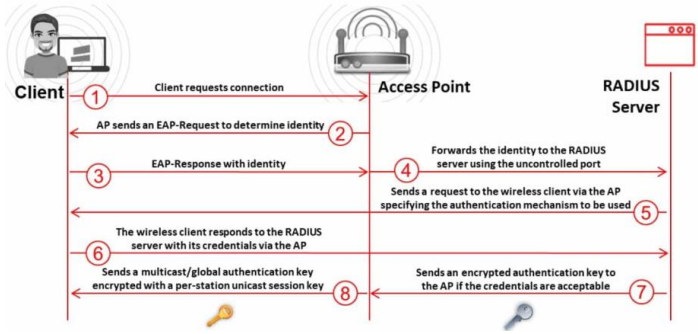
1. Mode PSK

- Le Pre Shared Key, connu sous le nom WPA-PSK ou WPA2-PSK, permet de sécuriser le wifi par un unique mot de passe partagé pour authentification.



2. Mode authentification centralisé

- Repose sur un serveur d'authentification RADIUS qui valide les identifiants des utilisateurs.



Sécurisation du réseau Wifi

V. Sécurisation du réseau Wifi

1. Sécurisation du AP

- Changer les mots de passe par défaut du point d'accès.
- Désactiver les services inutiles (telnet, snmp, …)
- Régler la puissance d'émission au minimum nécessaire.
- Mettre à jour le « Firmware » du point d'accès.
- Sécuriser l'accès physique vers les points d'accès.

V. Sécurisation du réseau Wifi

1. Sécurisation du AP

- **Filtrage d'adresses MAC** : Pour filtrer les clients, L'AP doit vérifier si l'adresse MAC de la station qui cherche à s'authentifier se trouve bien dans une liste d'adresses MAC autorisées (White list).
- **Désactiver la diffusion du SSID** (Service Set Identifier) : Par défaut, il est diffusé publiquement pour permettre aux appareils de le détecter. Masquer le SSID empêche les utilisateurs non autorisés de voir le réseau et réduire le risque d'attaque de type wardriving.

V. Sécurisation du réseau Wifi

2. Chiffrement WEP

- **W**ired **E**quivalent **P**rivacy est le premier chiffrement utilisé par le WiFi.
- Chiffrement symétrique des trames 802.11 utilisant l'algorithme RC4 avec des clés statique de 64 ou 128 bits.
- Les 24 premiers bits servent pour l'initialisation diminuant d'autant la taille de la clé.
- La clé doit être partagée par tous les équipements.
- Cet algorithme de chiffrement est très insuffisant.

V. Sécurisation du réseau Wifi

3. Chiffrement WPA

- Le chiffrement WPA « **W**iFi **P**rotected **A**ccess » repose sur des protocoles d'authentification et un algorithme de chiffrement robuste: **TKIP** (Temporary Key Integrity Protocol) qui introduit un chiffrement par paquet et la génération aléatoire des clés de chiffrement.
- On trouve deux versions **WPA personnel** et **WPA Entreprise**.
- WPA personnel repose sur l'utilisation des clés partagées **PSK** Pre-Shared Key, renseigné dans le point d'accès ainsi que dans les postes clients.
- La version personnelle du WPA-PSK ne prend en charge que les réseaux en mode infrastructure.

3. Chiffrement WPA

- Le **WPA Entreprise** impose l'utilisation d'un serveur d'authentification, généralement un serveur **Radius** (Remote Authentification Dial-in User Service) selon la norme **802.1x**, permettant d'identifier les utilisateurs et de leur définir des droits.
- Une version restreinte du protocole est appelée WPA-PSK (Pre-Shared Key) nécessitant de déployer une même clé (pass phrase) pour tous les équipements pour s'authentifier.
- Une fois l'authentification réussie, le **4-Way Handshake** entre le client et l'AP génère une clé de session unique pour chaque utilisateur pour chiffrer la communication

4. Chiffrement WPA2

- La norme 802.11i a été approuvée le 24 juin 2004.
- La certification WPA2 a été créée par la Wi-Fi Alliance.
- Le WPA2 offre un choix du cryptage, entre le **TKIP** et l'algorithme **AES-128** (Advanced Encryption Standard).
- Le chiffrement WPA2 est vulnérable à l'attaque **KRACK** (Key Reinstallation Attack), qui permet à un attaquant d'intercepter le trafic entre une station et un point d'accès et exploiter une vulnérabilité durant le 4-Way-Handshake.

V. Sécurisation du réseau Wifi

5. Chiffrement WPA3

- Dernière norme de sécurité pour les réseaux Wi-Fi
- Lancé en 2018 par la Wi-Fi Alliance
- Protection renforcée contre les attaques par force brute / dictionnaire
- Wifi public sécurisé : sans mot de passe, WPA3 chiffre la communication.
- Chiffrement renforcé AES-256 :
  - Clés de chiffrement plus longues : Moins vulnérable aux attaques.
  - Moins d'impact sur les performances : Chiffrement plus rapide et efficace.
- Incompatibilité avec les anciens appareils.

V. Sécurisation du réseau Wifi

6. La Norme 802.1X

- Pour palier aux lacunes de sécurité du 802.11, l'IEEE propose **802.1x** qui est une architecture basée sur **EAP**.
- La norme 802.1x propose un protocole d'authentification réseau sécurisé et offre une solution de gestion dynamique des clés.
- EAP (**E**xtensible **A**uthentication **P**rotocol) : est une solution d'authentification réseau flexible et robuste.
- La norme 802.1x utilise les protocoles : EAP-TLS, EAP-TTLS, EAP-MD5, PEAP,… pour une utilisation des mots de passe, des Hash et des certificats.

6. La Norme 802.1X – Méthodes d'authentification

Méthode EAP	Caractéristiques
EAP-TLS	Impose l'utilisation d'un certificat côté client et serveur
EAP-TTLS	Tunnel sécurisé (TLS) est créé entre client (n'a pas besoin d'un certificat) et serveur (présente un certificat pour prouver son identité)
EAP-MD5	principe qui repose sur un challenge-réponse en utilisant un hash du mot de passe.
PEAP	Consiste à envoyer l'identifiant et le mot de passe du client dans un tunnel sécurisé (TLS)

Evaluation des connaissances

V. Evaluation des connaissances

Question n° 1

- Lequel des moyens suivants est utilisé pour sécuriser une connexion WPA2 ?
  - A. WEP
  - B. AES (Advanced Encryption Standard)
  - C. MD5
  - D. SSL/TLS

Question n°2

- Quelle est la principale faiblesse du protocole WEP :
  - A. L'absence de protection contre les attaques par force brute.
  - B. L'incompatibilité avec les réseaux modernes.
  - C. La difficulté à configurer.
  - D. L'utilisation de clés statiques de petite taille.

V. Evaluation des connaissances

Question n° 3

- Le mode WPA2-Entreprise repose sur quelle méthode pour authentifier les utilisateurs :
  - A. Une clé pré-partagée (PSK).
  - B. Un serveur RADIUS.
  - C. Une adresse MAC.
  - D. Un identifiant unique sur chaque appareil.

Question n° 4

- Lequel de ces protocoles est considéré comme obsolète en raison de ses faiblesses de sécurité ?
  - A. WPA2
  - C. WPA3
  - B. WPA
  - D. WEP

V. Evaluation des connaissances

Question n°5

- Pourquoi WPA2 est-il préféré à WPA ?
  A. WPA2 est plus facile à configurer.
  B. WPA2 utilise AES, qui est plus sécurisé que TKIP utilisé par WPA.
  C. WPA2 a un meilleur signal Wi-Fi.
  D. WPA2 ne nécessite pas de mot de passe.

V. Evaluation des connaissances

Question n°6

- Une entreprise a configuré son réseau Wi-Fi en WPA2-Entreprise avec un serveur RADIUS. Cependant, elle veut permettre à certains employés en déplacement d'accéder au réseau à distance en toute sécurité. Quelle serait la meilleure option pour permettre cet accès sécurisé ?
  A. Donner le mot de passe PSK du réseau aux employés concernés.
  B. Configurer un VPN (Virtual Private Network) pour sécuriser les connexions à distance.
  C. Utiliser WEP pour les connexions à distance, car il est plus facile à configurer.
  D. Créer un réseau Wi-Fi ouvert uniquement pour les employés en déplacement.

V. Evaluation des connaissances

Question n°7

- Une entreprise remarque que des appareils non autorisés se connectent à son réseau WiFi. Quelle pourrait être la cause ?
  - A. Un employé a partagé le mot de passe WiFi
  - B. Un attaquant a installé un Rogue Access Point
  - C. Une attaque par force brute a deviné le mot de passe WiFi
  - D. Toutes ces réponses

V. Evaluation des connaissances

Question n°8

- Quel est le principal rôle de la norme 802.1X ?
  - A. Chiffrer automatiquement toutes les connexions WiFi
  - B. Accélérer la vitesse des connexions sans fil
  - C. Contrôler l'accès réseau via une authentification centralisée
  - D. Remplacer l'authentification par mot de passe

V. Evaluation des connaissances

Question n°9

- Un administrateur réseau d'entreprise découvre qu'un employé a configuré un routeur personnel au bureau pour étendre la couverture WiFi. Quel est le principal risque ?
  - A. L'entreprise pourrait être facturée pour l'utilisation du routeur
  - B. Le routeur peut être compromis et devenir un Rogue Access Point
  - C. La connexion WiFi sera plus rapide pour tout le monde
  - D. Il n'y a aucun risque

V. Evaluation des connaissances

Question n°10

- Comment 802.1X empêche-t-il un attaquant de s'authentifier en usurpant une adresse MAC légitime ?
  - A. En filtrant automatiquement les connexions suspectes
  - B. En forçant les utilisateurs à changer régulièrement leur mot de passe
  - C. En limitant le nombre d'appareils pouvant se connecter simultanément
  - D. En exigeant un certificat ou des identifiants uniques pour chaque utilisateur

V. Evaluation des connaissances

Question n°11

- Quel mode d'EAP est le plus sécurisé pour l'authentification sur 802.1X ?
  - A. EAP-MD5
  - B. EAP-TLS
  - C. EAP-LEAP
  - D. PEAP

V. Evaluation des connaissances

Question n°12

- Quel protocole est utilisé avec 802.1X pour gérer l'authentification ?
  - A. SNMP
  - B. SSH
  - C. HTTPS - TLS
  - D. EAP