Wi-Fi Security

M. Abbas Attoum

25/01/2019

### Introduction:

3h de cours

3h de pratique

**Entreprise :**

Client, Fournisseur, Operateur, …

**Poste :**

* R&D : Développe le logiciel
* Support : Suit les tickets des clients et fix le logiciel
* Avant-vente : technique et relationnel : fonctionnalité
* Commercial : Discute, finalise le deal

# Wireless : Infrastructure

Base stations: relay traffic between wireless and wired networks

* Cell tower
* Access point
* …

**Access network :** you access the network through wireless connections

Infrastructure mod:

Ad. hoc mode = no base station

## Characteristics of wireless links :

802.11 = WiFi standardised by IEEE, group of researchers

802.3 = Ethernet

802.15 = Bluetooth

IETF does the standards

802.11aw = 2019, last released

What is the minimum Rate necessary for voice

To transform a voice to digital

Fe >= 2Fmax

Voice frequency from 0 to 4000 Hz

Fe = 8000 Hz, sample per second

Each value is from -127 + 127

So on 8 bits so a Byte

8000 \* 8 = 64 000 b / s = 64 Kb / s = 8 KB /s without compression

Wifi benefits :

* Mobility
* Compatibility with IP networks
* Security

We can’t transmit at the same frequency ⇒ collisions

# 802.11 architecture

OSI model : Physical Layer + Data Link layer

### Physical layer

* 2.4GHz / 5 GHz
  + License free
* Different channels (frequencies)
  + Europe :13 channels
  + USA : 11 channels
* **MIMO :** multiple inputs, multiple outputs (talking at different people at the same time, or different people talking to 1 guy at the same time)

### DataLink layer

* **RTS** = request to send
  + Before sending a huge amount of data, you send a small one
* **CTS** = clear to send
  + Reply. “It’s okay to send”.

This avoids collisions.

## Beacons / association

**Association** = when you connect to a wifi network.

* You’re allowed to have your packets transmitted

AndroidAP as default Android hotspot (Access Point) SSID (name) so if connected to one before will try to connect to it automatically.

Passive scanning :

* Beacon frames sent from APs
* Association request frame sent : HI to select AP
* Association response frame sent from selected AP to Hi

Active scanning :

IBBS :

Without a access point ad hoc

BBS : basic service set =

Use an access point for the network

ESS : Extended service Set = set of one or more BBS (part of a network. Sever access point, interconnected. They communicated through a station)

Media access Control

* Scanning
* Authentification
* Association
* Encryption
* RTC-CTS
* Power safe mode
* Fragmentation

1. The station finds AP1, it will authenticate and associate
2. As the station moves, it may pre(authenticate with AP2
3. When the association with AP1 is no longer desirable, it may reassociate with AP2
4. AP2 notify AP1 of the new location of the station, terminates the previous association with AP1
5. At some point AP2 may be taken out of service. AP2 would dissociate the associated

802.11 frame addressing:

* 3 mac addresses : AP, Client, Router

**Frame subtypes :**

* **Control :** controls the scheduling (ordonnancement). We allocate to each source an access (/function of time, frequency)
* **Data :** between two access points
* **Management :** Beacon, Probe Request & Response, Authentification, De-authentification, … (between access point and access point controller)

# Security

Different features :

* **Association**
* **Authentication =** either opened or closed
* **Access control =** access point can decide which clients are allowed to associate based on MAC address
* **Data integrity =** data can’t be modified on the fly. Guaranteed by encryption.
* **Data confidentiality =** data eavesdropping with decryption of data. Guaranteed by encryption.
* **Encryption**
  + WEP (insecure)
  + WPA (insecure)
  + WPA2 (recommended)
  + WAPI (for China)

### Wired Equivalent Privacy = (WEP)

* First, optionally authenticate users
* Second, let’s at least try to encrypt every packet
* Authenticate with shared key allows
  + First send ket
    - Clear
    - Can be sniffed
  + Second idea
    - Num & hash
    - Access point also computes hash
    - = Instant replay
  + Third idea
    - Client sends intention
    - Access point send one random number
    - Client hash with number and key

### WEP encryption and decryption

* We have a pre-shared key + We choose an init vector (IV header) that we put in the frame = RC4 algorithm
* XOR it on plain information
* Send it

### WEP Integrity check

Create Integrity Check Value

* Added after Encrypted payload
* Has to be the same on arrival

### WAP

**AAA**  authentication, authorization, accounting

**WPA-TKIP** : temporal key

Generate a new encryption key for each new client

### WAP2

* Use AES instead of RC4

**Ieee 802.1X = radius**

* Uses EAP (Extensible authentication protocol): how to secure authentication
  + NAS = network access service // point d’accès

## Practical work

<https://manage.wifioncloud.com:8443/wsg/>

zone

Admin123!

Address mac : private on my local network

Retracer en local. Combien de temps logs stocké? Imposé par la loi : 12 ou 24 mois en fonction des pays. ⇒ min 5 ans en général

Pays où le trafic est surveillé

Volonté d'utiliser un vpn pour protéger ses données

Si Vpn ports bloqués ⇒ rediriger vers un autre port (80)

Deep packet inspection (dpi) ⇒ même si passe par autre port dans l’en tête vpn on peut savoir que c’est un trafic vpn

⇒ on regarde au coeur ⇒ on voit les protocoles vpn

⇒ on encapsule vpn dans un packet ssh ou https car crypté car l’entête vpn sera cryptée (443, 22)

Ou alors si tout internet est bloqué, peut toujours passer par les ports toujours ouvert sinon rien ne marche (contourner l’internet payant)

Dhcp : 67

Dns : 53

Pour remédier à cela dans le firewall

DHCP : Bloquer au niveau du firewall pour le dhcp puisque c’est interne donc on ne passe pas par le firewall

DNS : port 53 **ET** ip au niveau du firewall

Différents annuaires :

* SQL
* AD (LDAP)

Login radius :

ece\_1

1463