

WIRELESS LOCAL AREA NETWORK SECURITY



Jesús Gil Cabezas - i62gicaj@uco.es

www.yisux.wordpress.com



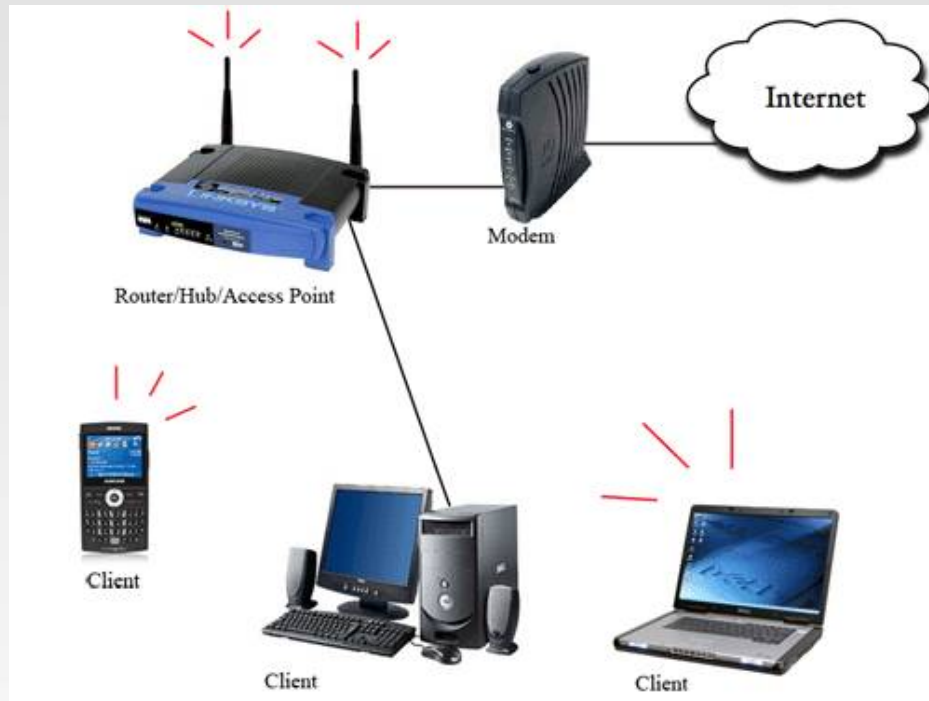
WIRELESS LOCAL AREA NETWORK SECURITY



■ Index

- WLAN
 - Advantages
 - Disadvantages
 - Security
- WLAN CRACKING

WHAT IS A WLAN?



■ WLAN

- **Wireless Local Area Network**
- **First Wireless Data Modems were developed in 1980s by amateur radio**
- **Other Wireless communication called Bluetooth was developed in 1995.**
- **In 1997 released the first WLAN when IEE (Institute of Electronics and Electrical Engineer) published 802.11 standard.**
- **Architecture of a WLAN**

HOW WLAN WORKS?



■ WLAN

- **Wi-Fi Technology uses radio waves.**
- **Aim: provide wireless access to digital content**
- **Internet signal plug in a Router**
- **Router sends wi-fi signal with some features.**
- **Client receives signals in his range**
- **Introduce valid data features in order to connect with Router**
- **Packets of Data are transmitted between both.**

ADVANTAGES OF WLAN



- **ADVANTAGES**
 - **Mobility** → no wired network
 - **Expandibility** → increasing number of clients
 - **Low Cost** → no wires
 - **Entertainment** → videogames
 - **Businness** → conferences

DISADVANTAGES OF WLAN



- **DISADVANTAGES**
 - **Security** → vulnerabilities
 - **Range** → limited
 - **Speed** → lower than wired
 - **Waves troubles** → interferences

WLAN SECURITY



■ WLAN Security

- Encryption → OPEN, WEP, WPA, WPA2...
- Now it is recommended use WPA or WPA 2 if it is possible.
- Hackers can obtain encryption password
- Free Internet Connection
- Steal data of victim's computer
- It is illegal

WLAN CRACKING



- **WLAN CRACKING**
 - Programs → Obtain password
 - GNU/Linux Distribution
 - WEP → Cracked
 - WPA → Cracked
 - How is possible?
 - Different Methods



- **PROGRAMS & GNU/LINUX DISTROS**
 - **Aircrack-ng**
 - **Airodump-ng**
 - **Aireplay-ng**
 - **GNU/Linux Distros**
 - **Backtrack**
 - **WifiWay**
 - **WifiSlax**

[Aircrack-ng website](http://www.aircrack-ng.org)

<http://www.aircrack-ng.org/doku.php?id=aircrack-ng.es&do=backlink>

WEP & WPA CRACKING



■ WEP & WPA CRACKING

■ WEP

- Valid Data Packets
- Number of Packets
- Cracked by users

■ WPA

- Valid Data Packets
- Number of Packets
- Dictionary
- Cracked by users with a good dictionary

HOW IS POSSIBLE?



■ HOW IS POSSIBLE?

- Victim Network
 - Data Traffic
 - Vulnerable Encryption
- Attackant Client
 - Compatible Hardware
 - Aircrack-ng software
 - Fake authentication
 - Catch Valid Data Packets
 - Search and decrypt password

Compatible Hardware List

http://www.aircrack-ng.org/doku.php?id=compatibility_drivers

DIFFERENT METHODS

■ DIFFERENT METHODS

■ WEP

- With injection
- Without injection
- 100% cracked with sufficient Valid Data Packets

■ WPA-WPA2

- With injection
- Without injection
- Dictionary
- 100% cracked without dictionary last month by a professional



YOU MUST TAKE ATTENTION

- **For a secure WLAN**
 - **WPA-WPA2 Encryption if it is possible**
 - **Change the password once time a month**
 - **MAC filter**
 - **Traffic Viewer**
 - **Encryption of shared directories and files**



WIRELESS LOCAL AREA NETWORK SECURITY

Thanks!

