TRABAJO FIN DE GRADO

Análisis de amenazas y vulnerabilidades de seguridad en redes WiFi

Alumno: Ricardo José Ruiz Fernández

Tutor: D. Víctor Abraham Villagrá González

Julio 2015

Objetivos

- Ver los aspectos generales de las redes WiFi

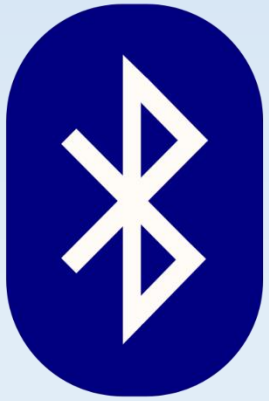
- Explicar cómo es la seguridad en esta tecnología

- Realizar pruebas de ataque a los distintos tipos de redes

- Ver qué herramientas de auditoría podemos utilizar

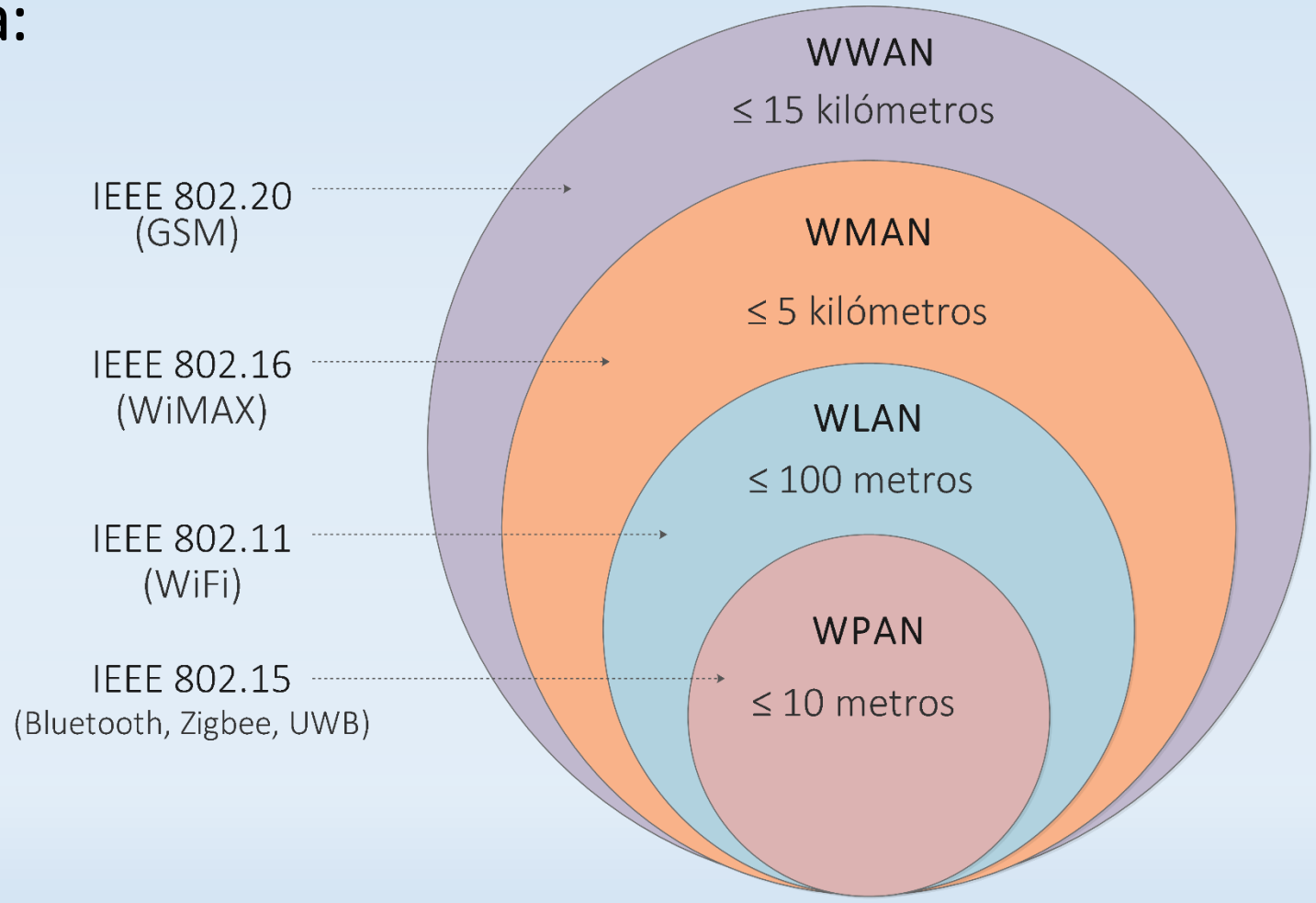
Las tecnologías inalámbricas

- Según tipo de tecnología:
  - Infrarrojos
  - Bluetooth
  - WiFi
  - WiMAX
- Según la cobertura:
  - WPAN
  - WLAN
  - WMAN
  - WWAN



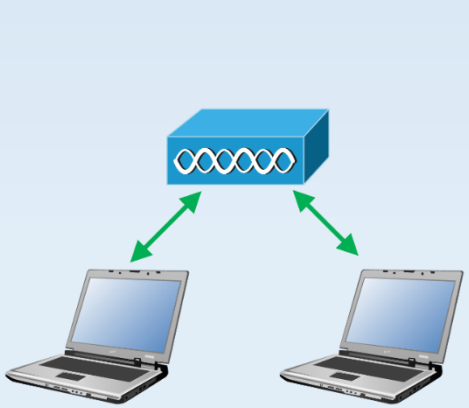
Las tecnologías inalámbricas

- Según tipo de tecnología:
  - Infrarrojos
  - Bluetooth
  - WiFi
  - WiMAX
- Según la cobertura:
  - WPAN
  - WLAN
  - WMAN
  - WWAN

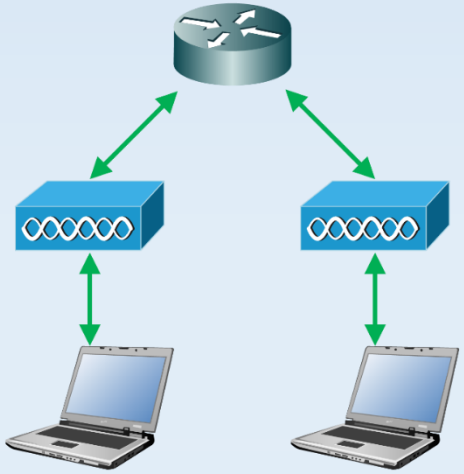


La tecnología WiFi

Modo infraestructura

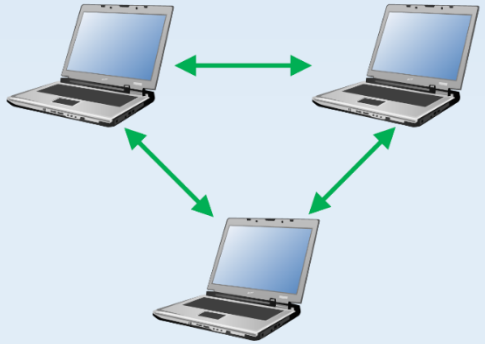


BSS



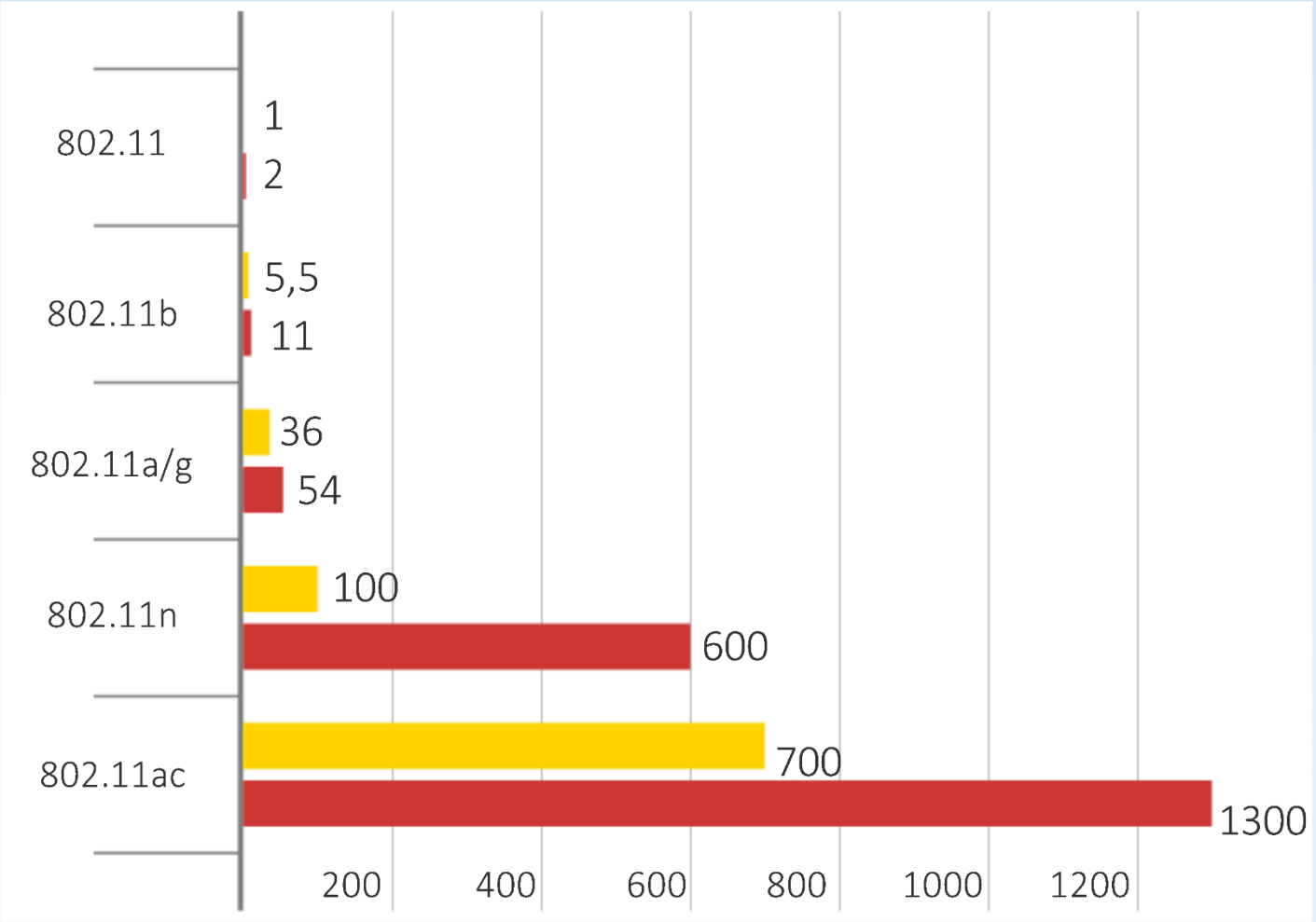
ESS

Modo Ad-hoc



IBSS

La tecnología WiFi



Seguridad en WiFi: Protocolos de protección

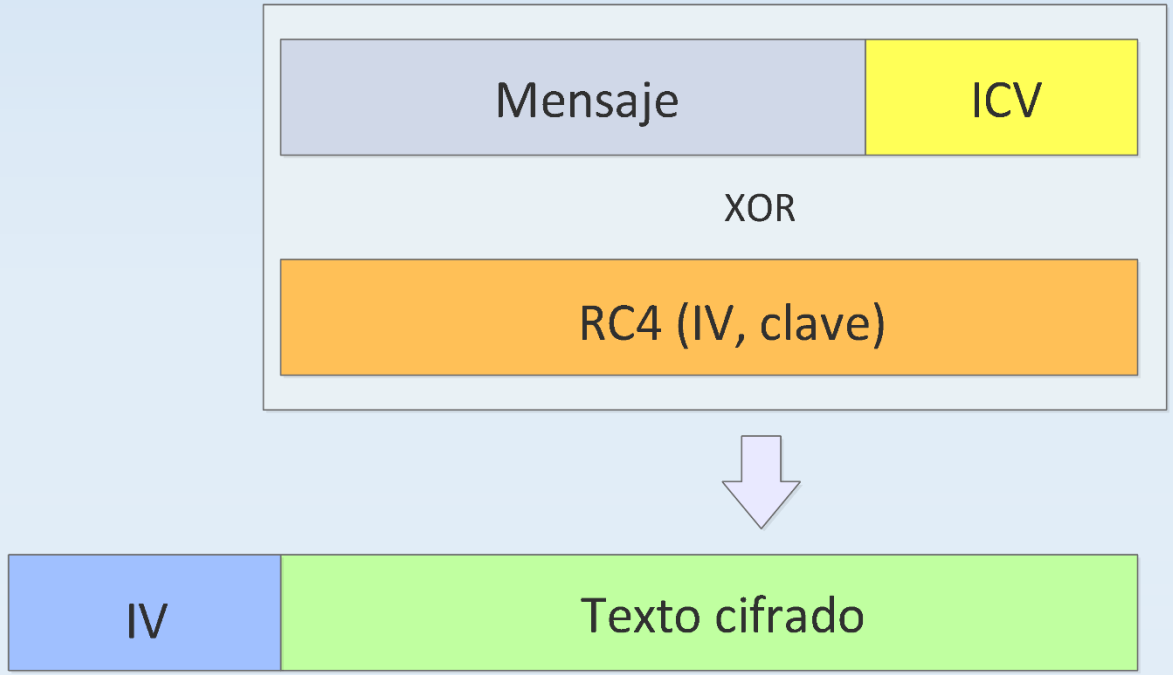
WEP ("Wired Equivalent Privacy")

- Autenticación
  - "Shared Key Authentication"
  - "Open System Authentication"
- Cifrado
  - Basado en el algoritmo RC4
  - Vector de inicialización (IV)
  - CRC-32: Código de integridad
- Vulnerabilidades: RC4, CRC-32, IV corto y repetido,…

Seguridad en WiFi: Protocolos de protección

WEP ("Wired Equivalent Privacy")

- Autenticación
  - "Shared Key Authentication"
  - "Open System Authentication"
- Cifrado
  - Basado en el algoritmo RC4
  - Vector de inicialización (IV)
  - CRC-32: Código de integridad
- Vulnerabilidades: RC4, CRC-32, IV corto y repetido,…



Seguridad en WiFi: Protocolos de protección

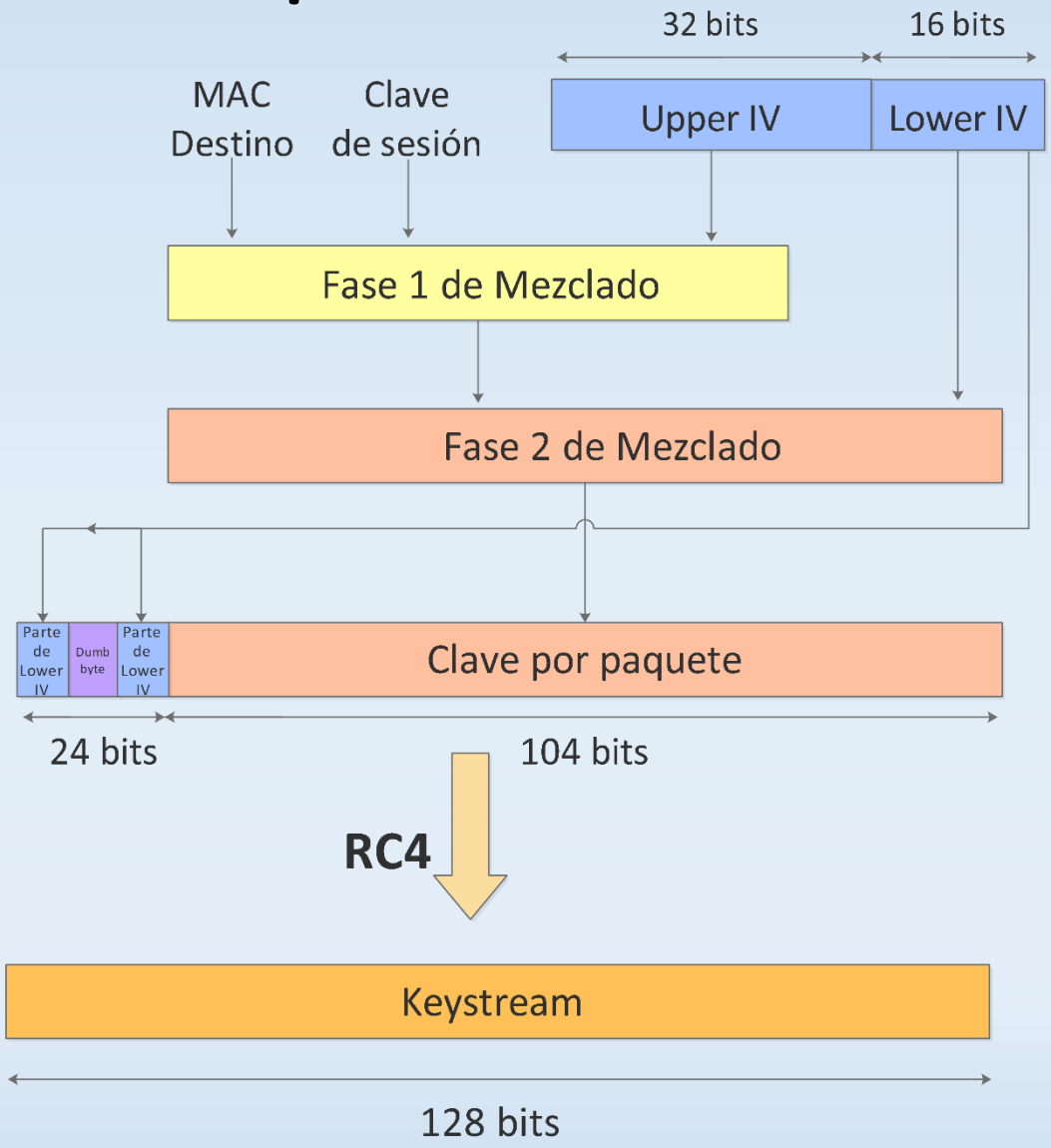
WPA (“WiFi Proteced Access”)

- Autenticación
  - WPA-PSK: Clave compartida
  - WPA-Enterprise: 802.1x EAP
- Cifrado
  - TKIP: Basado en RC4
  - IV mayor: De 24 a 48 bits
  - MIC: Nuevo código de integridad
- Vulnerabilidades: TKIP y WPS

Seguridad en WiFi: Protocolos de protección

WPA ("WiFi Proteced Access")

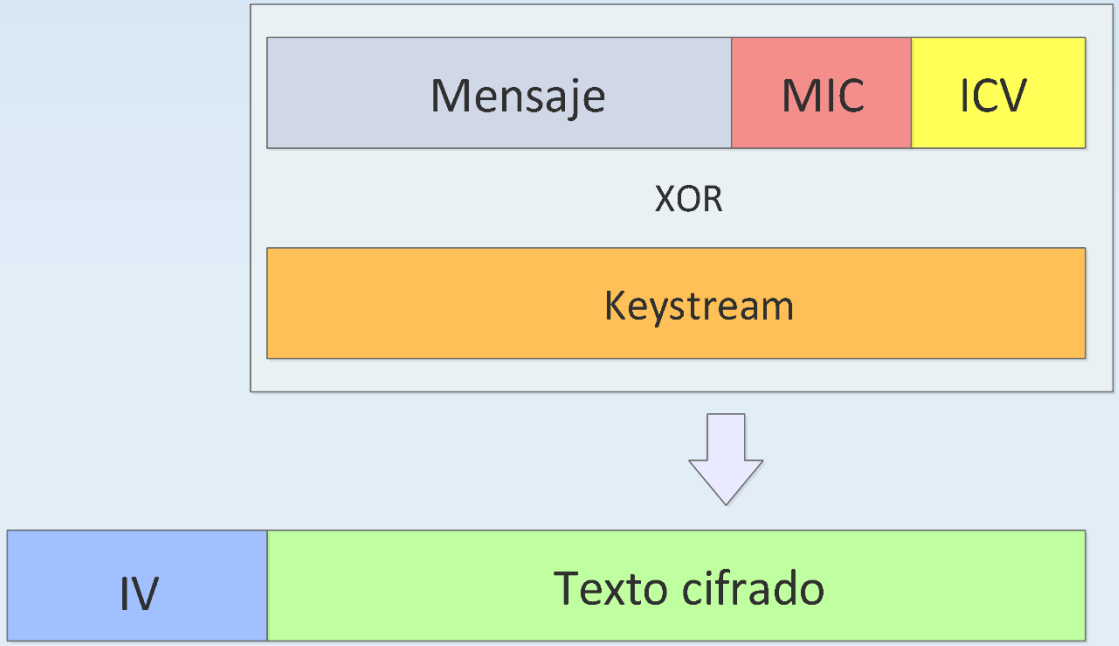
- Autenticación
  - WPA-PSK: Clave compartida
  - WPA-Enterprise: 802.1x EAP
- Cifrado
  - TKIP: Basado en RC4
  - IV mayor: De 24 a 48 bits
  - MIC: Nuevo código de integridad
- Vulnerabilidades: TKIP y WPS



Seguridad en WiFi: Protocolos de protección

WPA (“WiFi Proteced Access”)

- Autenticación
  - WPA-PSK: Clave compartida
  - WPA-Enterprise: 802.1x EAP
- Cifrado
  - TKIP: Basado en RC4
  - IV mayor: De 24 a 48 bits
  - MIC: Nuevo código de integridad
- Vulnerabilidades: TKIP y WPS



Seguridad en WiFi: Protocolos de protección

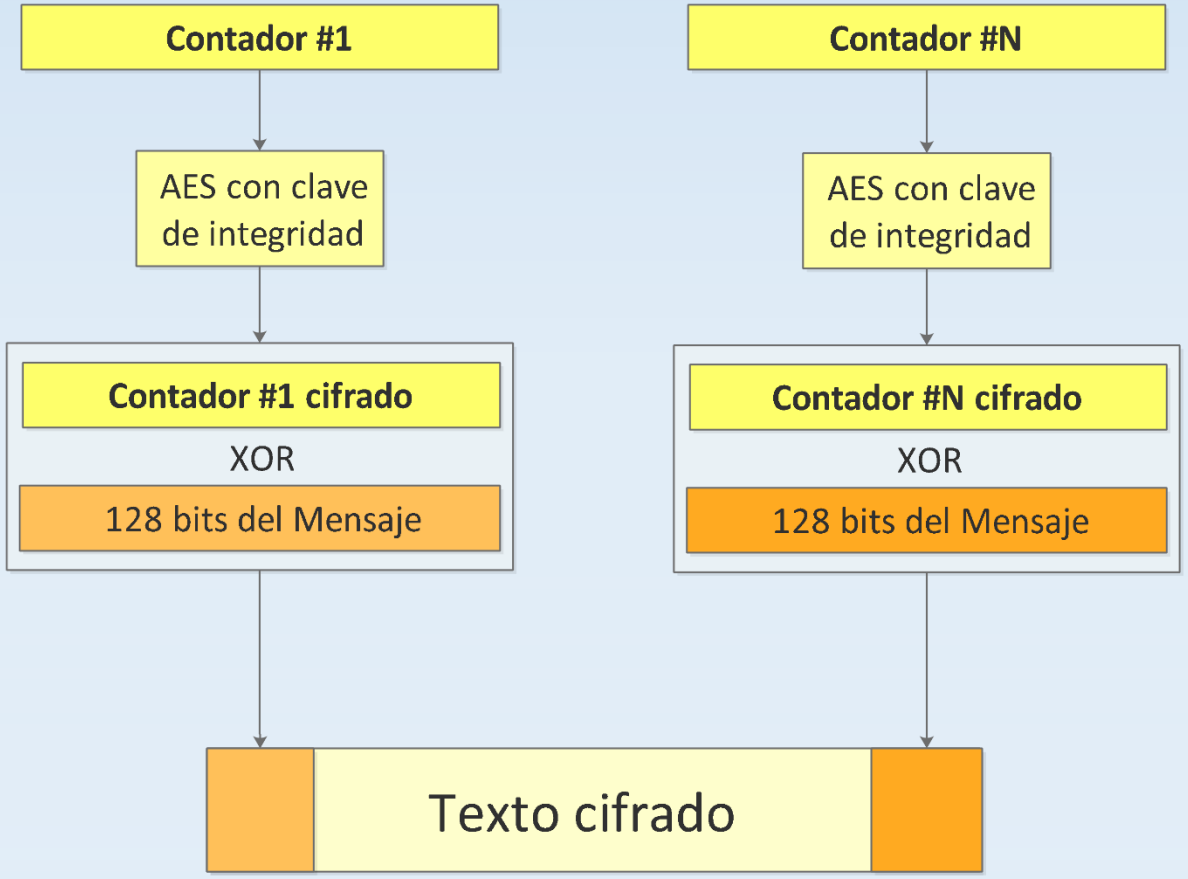
WPA2 (“WiFi Proteced Access 2”)

- Implementa 802.11i por completo

- Mismos modos y forma de autenticación

- Cifrado ⇨ CCMP (AES) { CBC-MAC, Counter Mode }

- Vulnerabilidad: WPS



Seguridad en WiFi: Protocolos de protección

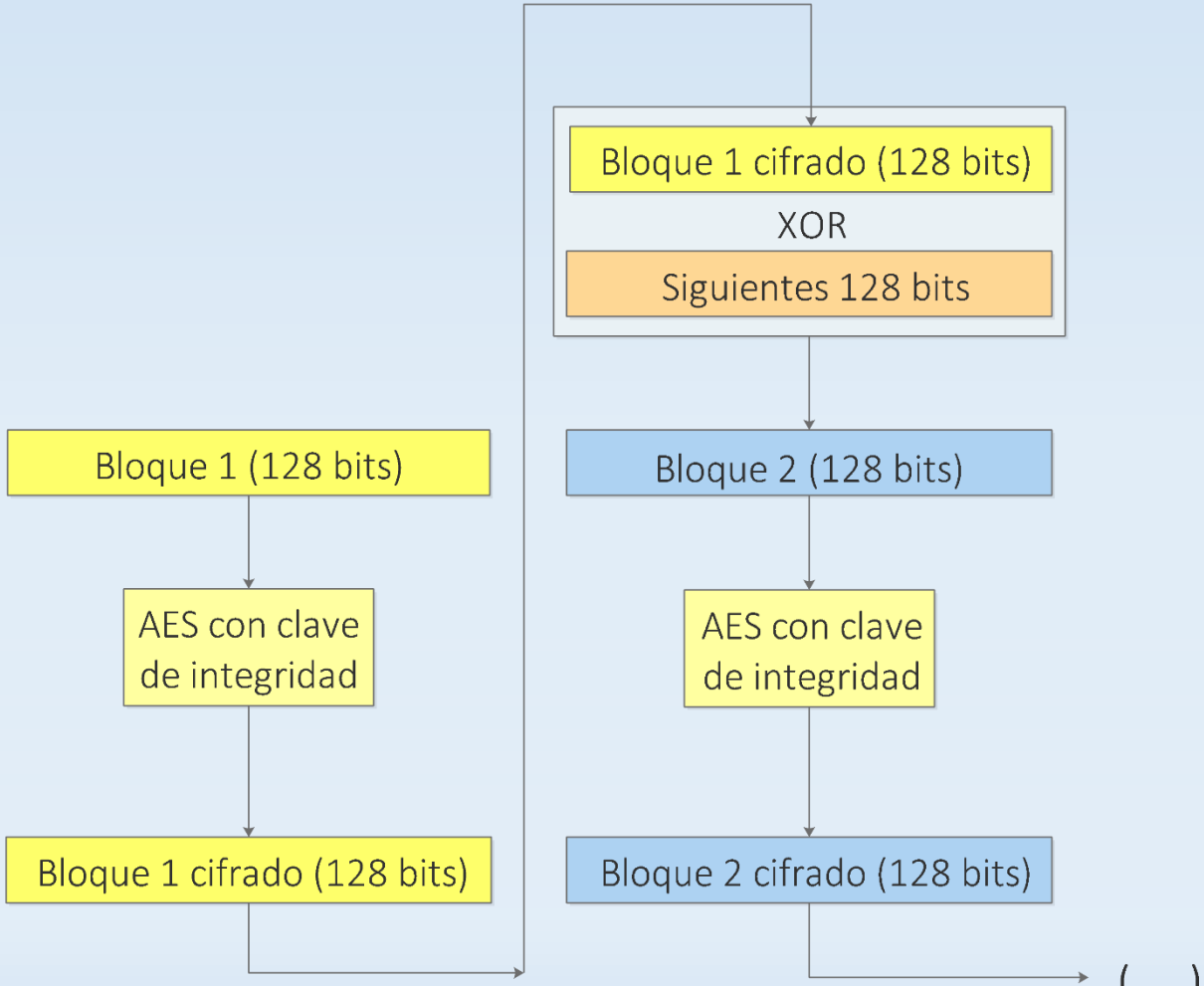
WPA2 (“WiFi Proteced Access 2”)

- Implementa 802.11i por completo

- Mismos modos y forma de autenticación

- Cifrado ⇨ CCMP (AES)
  - CBC-MAC
  - Counter Mode

- Vulnerabilidad: WPS



Seguridad en WiFi: Protocolos de protección

WPS (“Wi-Fi Protected Setup”)

- No es un protocolo, es un estándar

- Pensado para facilitar la autenticación

- Tipos
  - PBC (“Push-Button Configuration”)
  - PIN de 8 dígitos (11.000 posibilidades)

- Tres elementos: *enrollee, registrar* y *authenticator*

E => R	M1	N1 || Descripción || PKE
E <= R	M2	N1||N2||Descripción||PKR
E => R	M3	E-Hash1 || E-Hash2

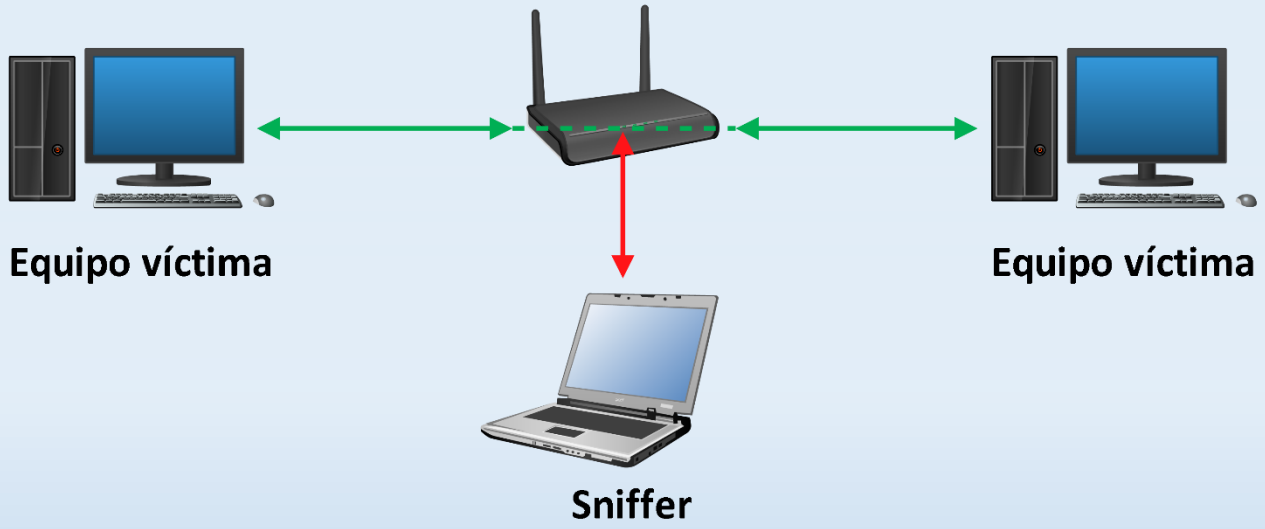
...

Seguridad en WiFi: Tipos de ataques

Ataques pasivos

- Análisis de datos: Controlar el tipo de tráfico, volumen, horario,…

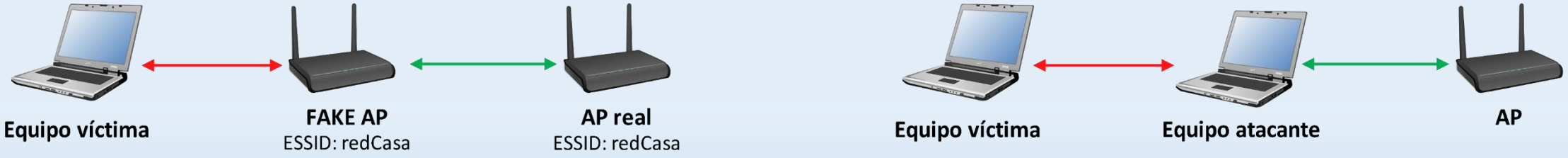
- Sniffing: Espiar el tráfico de una red para robar información comprometida.



Seguridad en WiFi: Tipos de ataques

Ataques activos

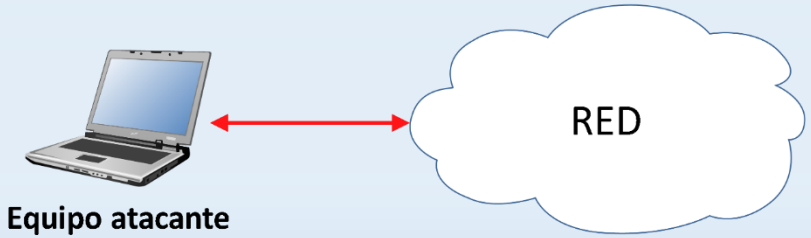
- Spoofing: Suplantación de un usuario o dispositivo de la red.
- Man in the Middle: Interceptación y/o modificación de tráfico.
- Inyección de paquetes: Capturar e introducir posteriormente parte de tráfico.
- Ataque de DoS: Inhabilitar un equipo (normalmente el AP).



Seguridad en WiFi: Tipos de ataques

Ataques activos

- Spoofing: Suplantación de un usuario o dispositivo de la red.
- Man in the Middle: Interceptación y/o modificación de tráfico.
- Inyección de paquetes: Capturar e introducir posteriormente parte de tráfico.
- Ataque de DoS: Inhabilitar un equipo (normalmente el AP).



Escenarios de ataque: Redes domésticas

Acceso no autorizado a la red

WEP

- IV repetidos => Aircrack-ng

  64 bits: < 3 minutos

  128 bits: < 8 minutos

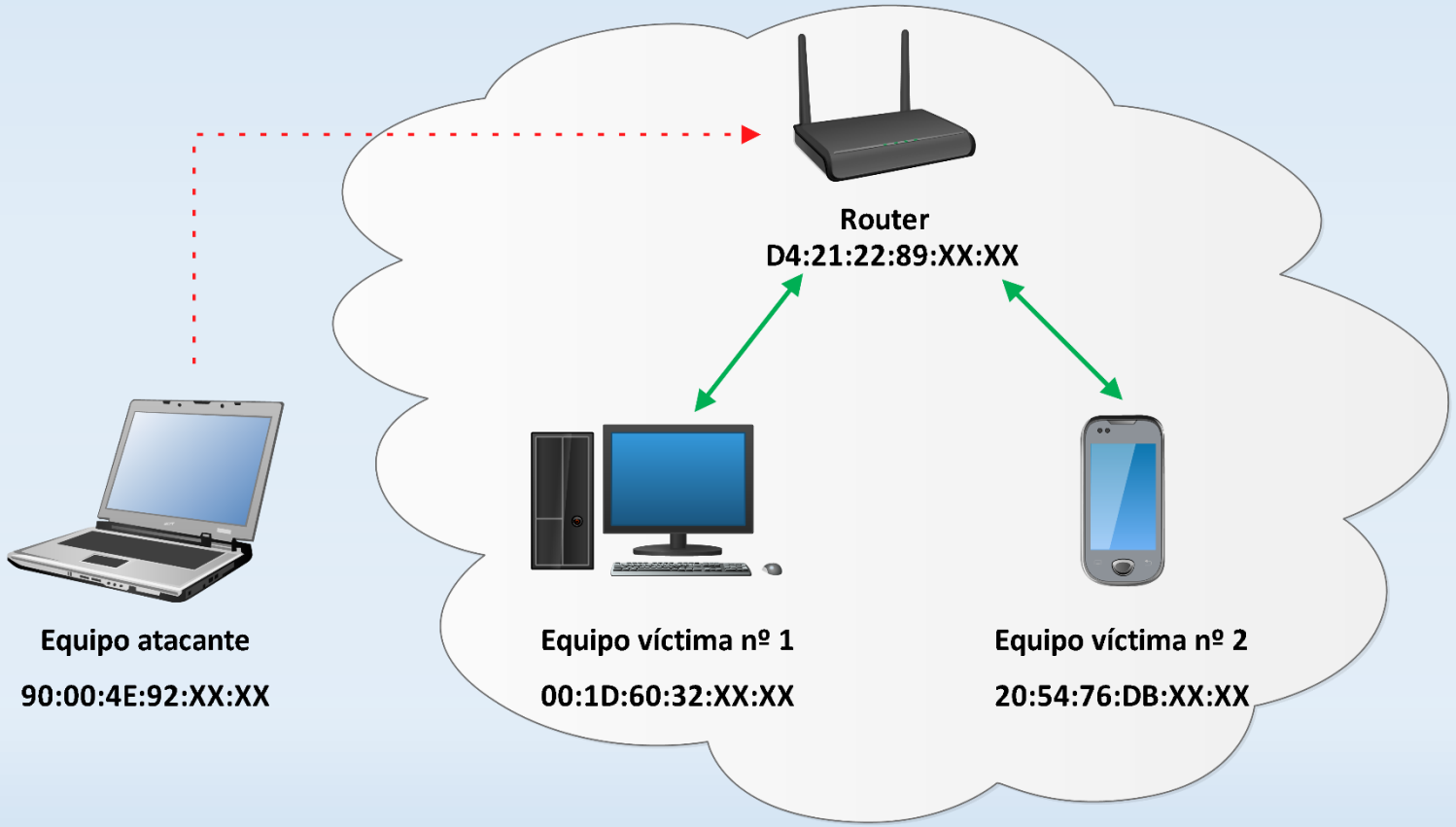
WPA-WPA2 con WPS

- Ataques online => Reaver

  Según router: ~ 12 horas

- Ataques offline => Reaver+Pixiewps

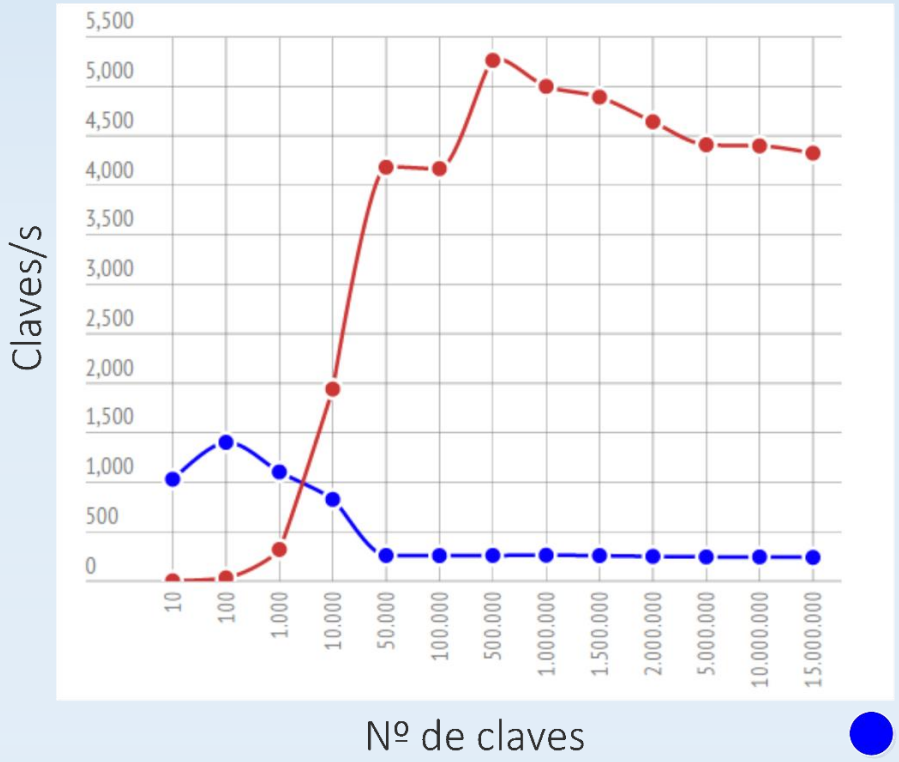
  Según chipset: < 1 minuto

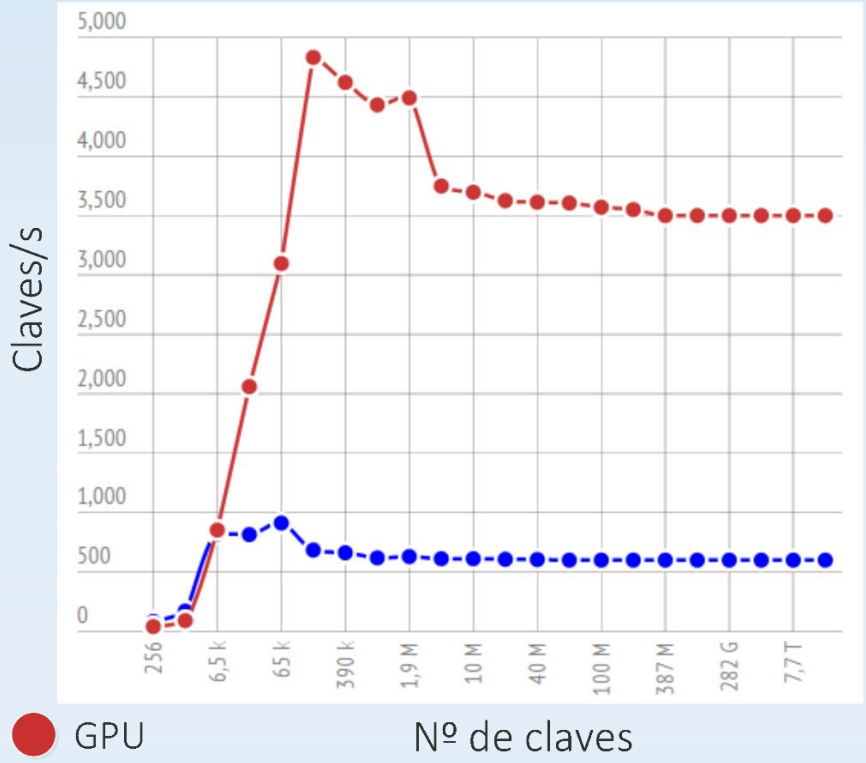


Escenarios de ataque: Redes domésticas

Acceso no autorizado a la red

WPA-WPA2 sin WPS





CPU GPU

Ataques de diccionario

Ataques de fuerza bruta

Escenarios de ataque: Redes domésticas

Ataque *Man in the Middle*

Paso 1: Busqueda de equipos

Nmap – Análisis de direcciones IP

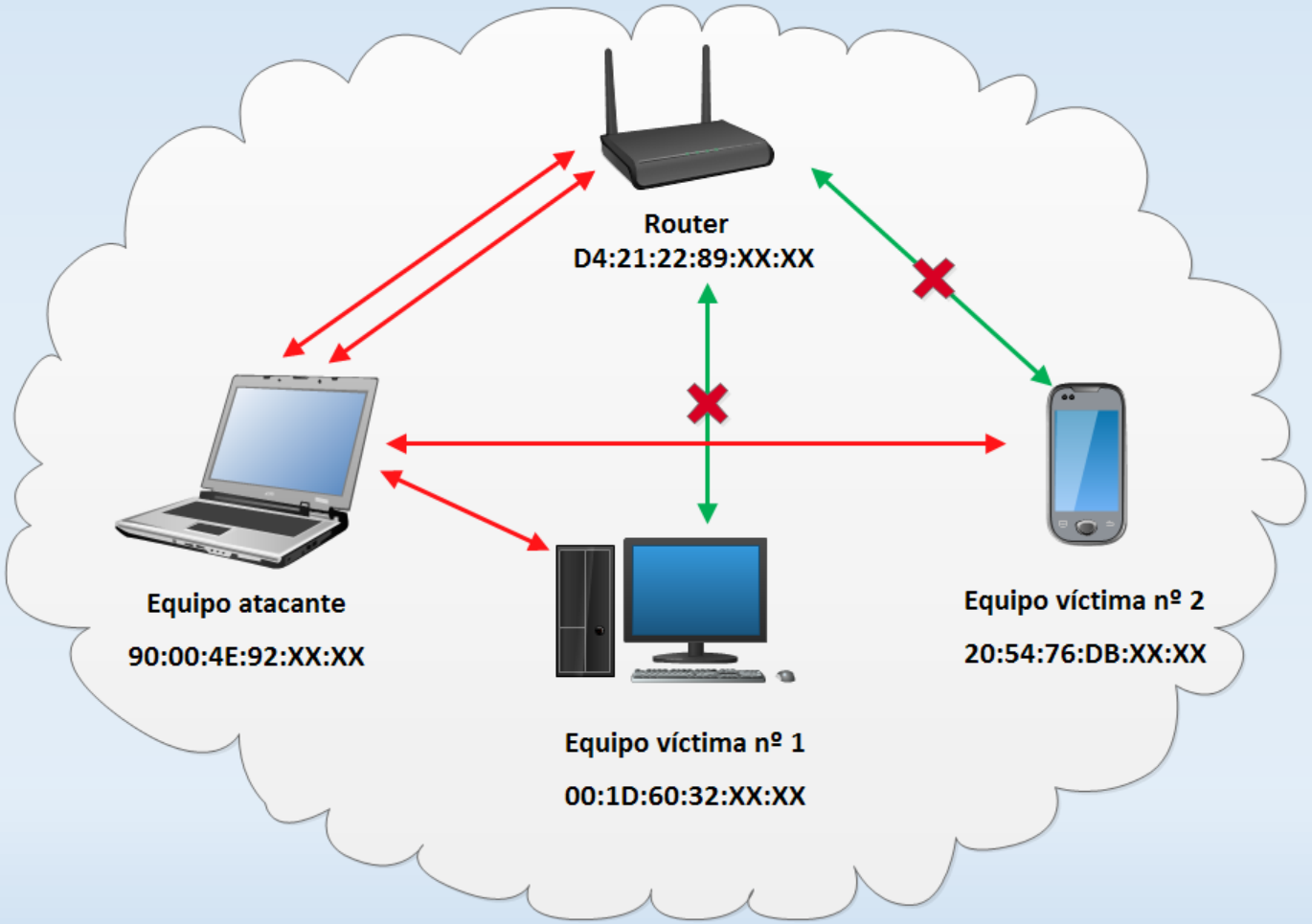
Paso 2: Envenenamiento ARP

Arpspoof – Tráfico a través del equipo

Paso 3: Sniffing

SSLStrip – Direcciones *https* => *http*

Ettercap
Wireshark
} Sniffing normal



Escenarios de ataque: Redes domésticas

Prototipo final

Paso 1: Acceso no autorizado

Obtener clave, protección, nombre

Paso 2: Ataque DoS

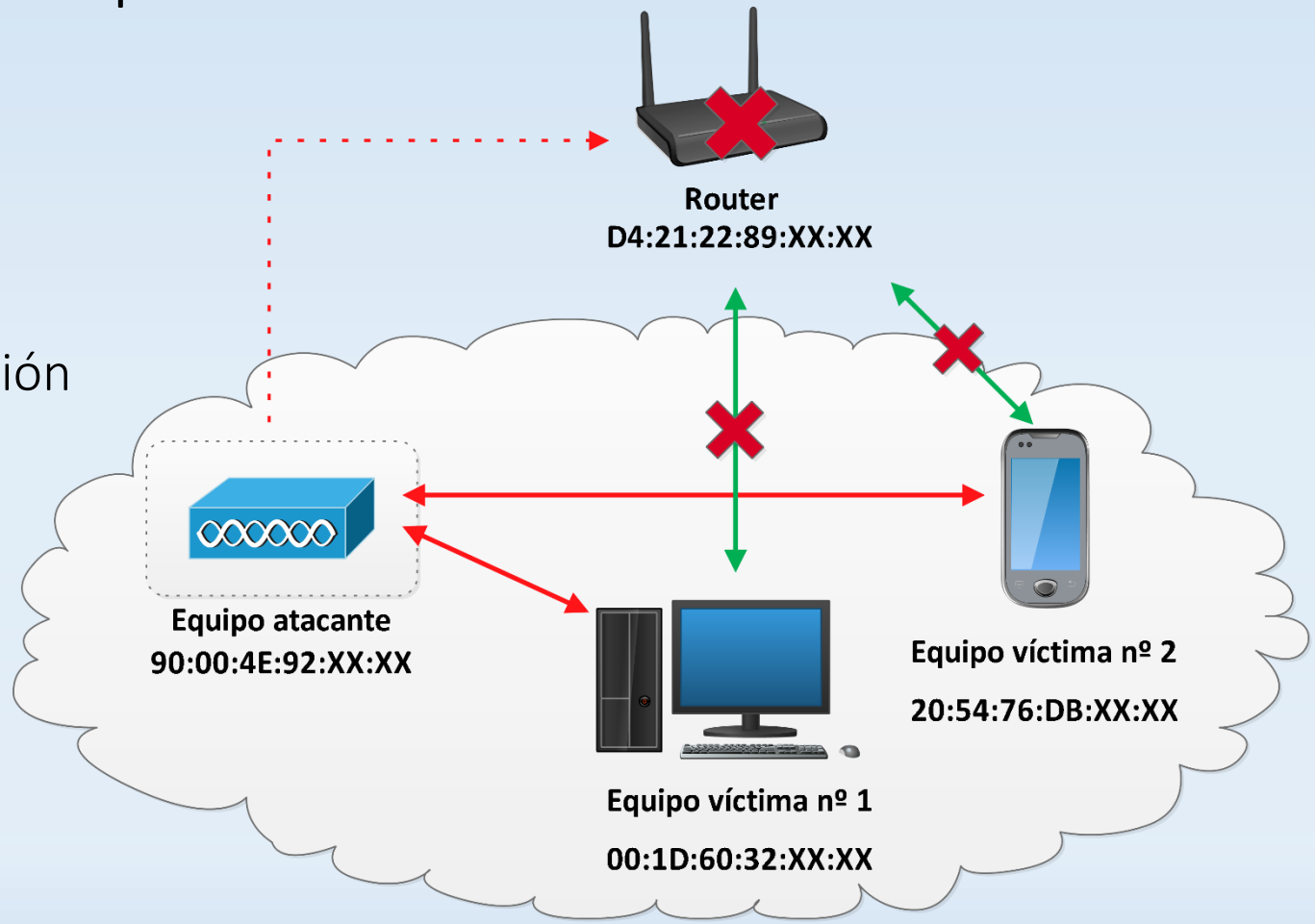
Aireplay-ng – Mensajes de desautenticación

Paso 3: Fake AP

Hostapd – Con la información del paso 1

Paso 4: MitM + Sniffing

SSLStrip + Ettercap + Wireshark



Escenarios de ataque: Redes empresariales

Obtención de credenciales

Paso 1: Configurar AP y servidor Radius

Antes de crearlos, podemos cambiar parámetros como la autenticación por defecto.

Paso 2: Crear Fake AP y servidor Radius

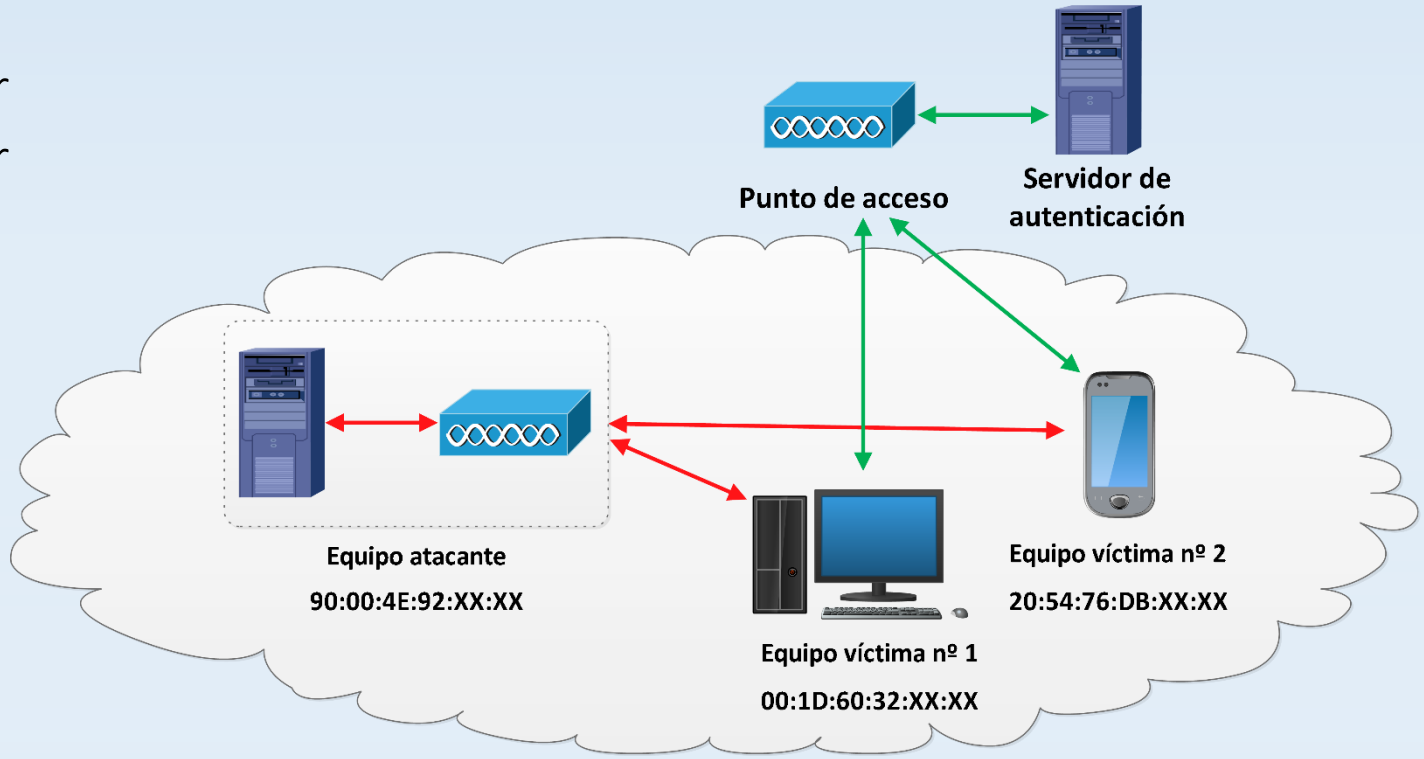
Hostapd: Crear el AP (con 802.1x)

Freeradius-WPE: Crear el servidor Radius

Paso 3: Obtener fichero con claves

EAP-MSCHAPv2 : Cifradas

EAP-GTC: En claro



Escenarios de ataque: Redes empresariales

Obtención de credenciales

Paso 1: Configurar AP y servidor Radius

Antes de crearlos, podemos cambiar parámetros como la autenticación por defecto.

Paso 2: Crear Fake AP y servidor Radius

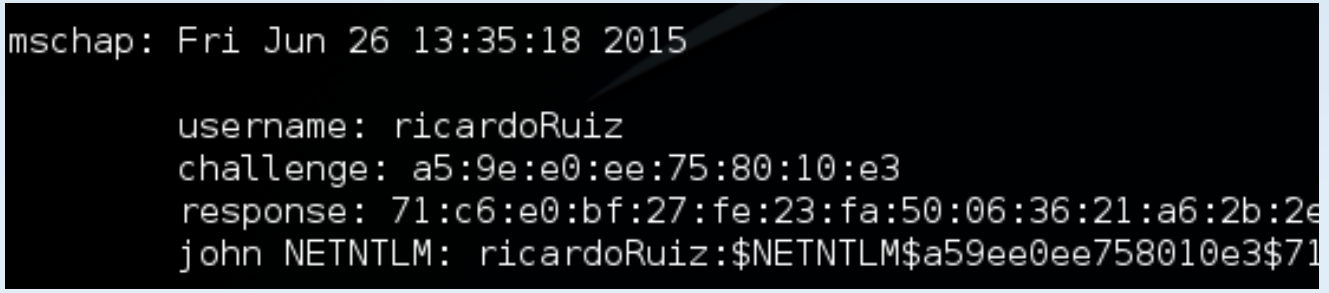
Hostapd: Crear el AP (con 802.1x)

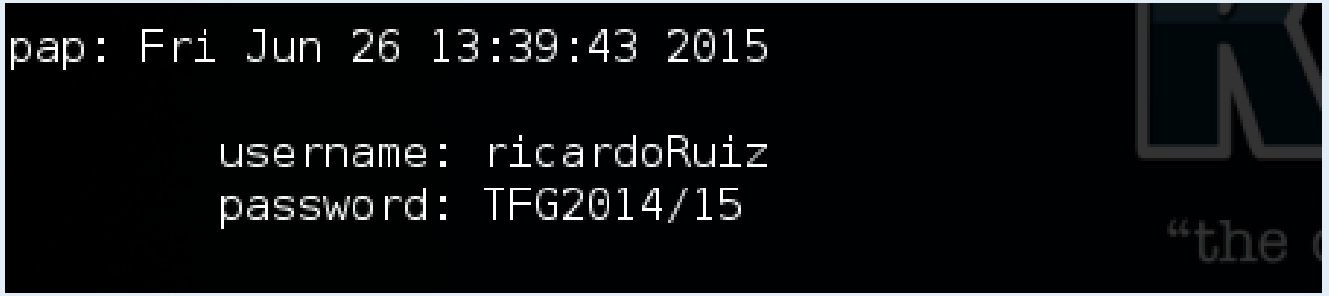
Freeradius-WPE: Crear el servidor Radius

Paso 3: Obtener fichero con claves

EAP-MSCHAPv2 : Cifradas

EAP-GTC: En claro





Escenarios de ataque: Redes empresariales

Prototipo final

Paso 1: Ataque DoS a APs cercanos

Paso 2: Configurar servidor Radius

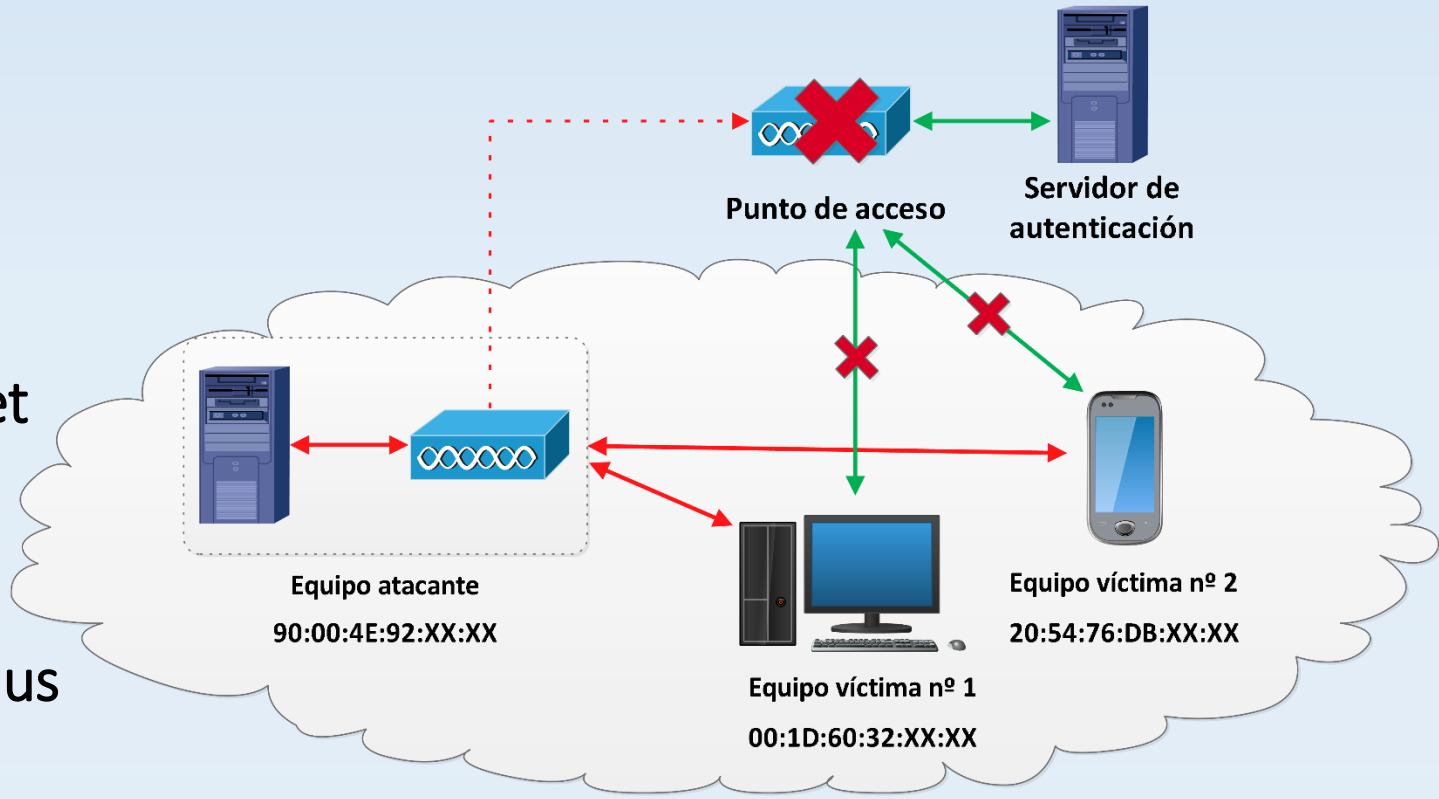
Permitimos que cualquier usuario pueda acceder.

Paso 3: Compartir conexión a internet

Con Iptables y Dnsmasq compartimos la conexión a internet con el Fake AP.

Paso 4: Crear Fake AP y servidor Radius

Paso 5: MitM + Sniffing



Escenarios de ataque: Redes empresariales

Pruebas en las redes de la ETSIT

3 redes con protección 802.1x EAP

1. ETSIT-WLAN: PEAP + MSCHAPv2
2. WIFIUPM
3. Eduroam

} TTLS + PAP

En los ordenadores: Instalar certificados

En móviles Android: No hace falta

Identidad: Nombre de su cuenta institucional
Identidad anónima: anonymous@upm.es
Contraseña: La contraseña asociada a la cuanta institucional.

Identidad: Nombre de su cuenta institucional
Identidad anónima: Dejar en blanco
Contraseña: La contraseña asociada a la cuanta institucional.

Escenarios de ataque: Redes empresariales

Pruebas en las redes de la ETSIT

3 redes con protección 802.1x EAP

1. ETSIT-WLAN: PEAP + MSCHAPv2
2. WIFIUPM
3. Eduroam

} TTLS + PAP

En los ordenadores: Instalar certificados

En móviles Android: No hace falta

```
mschap: Mon Jul  6 17:09:17 2015

        username: rruizfer12
        challenge: 6a:79:e6:61:16:fa:99:4a
        response: 1b:47:66:a7:5e:3d:34:c6:a8:8b:fa:ac
        john NETNTLM: rruizfer12:$NETNTLM$6a79e66116f
```

```
pap: Mon Jul  6 17:11:50 2015

        username: ricardo.ruiz.fernandez@alumnos.upm
        password: TFG2015
```

Conclusiones

- La seguridad en WiFi es muy importante
    - Las redes abiertas, protegidas con WEP o con WPS son peligrosas.
    - Con WPA2 podemos tener seguridad suficiente.
    - Hay autenticaciones inseguras en las redes empresariales.
- Líneas de continuación: Defender las redes WiFi de estos ataques