

# Tema-6-Seguridad-en-redes-inalam...



**adrian\_gutigoza**



**Seguridad en Redes**



**2º Grado en Ingeniería de la Ciberseguridad**



**Escuela Técnica Superior de Ingeniería Informática. Campus de  
Móstoles  
Universidad Rey Juan Carlos**



Estamos de  
**Aniversario**

De la universidad al  
mercado laboral:  
especialízate con los posgrados  
de EOI y marca la diferencia.



**EOI** Escuela de  
organización  
industrial



**saber más**

Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato  
→ Planes pro: más coins

pierdo  
espacio



Necesito  
concentración

ali ali ooh  
esto con 1 coin me  
lo quito yo...

WUOLAH



## Tema 6: Seguridad en redes inalámbricas

### PRINCIPALES PROBLEMAS DE LA SEGURIDAD WIFI Y CONTRAMEDIDAS

Las redes wifi son **redes inalámbricas**, por lo que su principal problema es que, al no existir un cable por donde puedan viajar los datos, el **medio de transporte es el aire**, **permitiendo a cualquier individuo ver el tráfico**. Debido a la naturaleza de la red se pueden producir ataques de Man in the Middle, Denegación de Servicio, Inyección de paquetes a la red, robo de identidad (MAC Spoofing)...

Para evitar estos problemas se pueden utilizar distintas **contramedidas** con mayor o menor nivel de efectividad:

- **Ocultación de la señal:** se busca poner los puntos de emisión de forma estratégica de forma que la **señal quede “encapsulada” en un área controlada**. Ej.: evitar que la señal wifi de una empresa en un edificio se extienda hacia la calle. También se **elimina el uso de las tramas beacon** de los routers para evitar publicitar la red. Contramedida poco segura.
- **Filtrado de equipos:** en el AP se filtra por las **MAC de los equipos** limitando la conexión a aquellos autorizados. Es poco seguro ya que con un MAC Spoofing se puede saltar rápidamente la restricción.
- **Políticas de seguridad:** una de las contramedidas más importantes. Ej.: formación de empleados, **campañas antiphishing**, **longitud de contraseñas...**
- **Autenticación:** los clientes se deben autenticar para poder conectarse a la red.
- **Cifrado:** es la contramedida estrella. Si se usa se evita que un tercero pueda interpretar nuestro tráfico que viaja por el aire. Ej. de cifrados: WEP, WPA, WPA2, WPA3

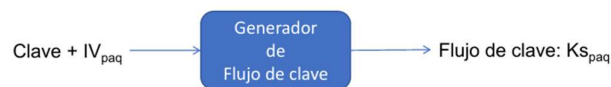
WUOLAH

## CIFRADO WEB (WIRED EQUIVALENT PRIVACY)

El **cifrado WEP** se basa en la **clave simétrica compartida** proporcionando así confidencialidad, integridad sobre los datos y autenticación. Se trata de un **cifrado no encadenado** por lo que el cifrado de un paquete no depende del anterior y si este se pierde se puede seguir descifrando. **Es eficiente** y se puede implementar mediante hardware o software. Hoy en día **es INSEGURO**.

### Cifrado simétrico de flujo

**WEP utiliza un cifrado de flujo (bit a bit)** RC4. Con una clave inicial se crea un flujo de clave pseudoaleatorio con el que se cifrará el mensaje. Para evitar que se use la misma clave para crear el flujo de clave lo que hace WEP es **uso de una clave** (siempre igual) y **un vector de inicialización IV distinto para cada paquete**, por lo que **se generará un flujo distinto para cada uno**.



### Cifrado WEP

1. El **emisor calcula un Integrity Check Value (ICV)** de los datos que ocupa 4 bytes. Es parecido a un hash.
2. Cada lado de la comunicación tiene una **clave compartida de 104 o 40 bits**
3. El **emisor crea un IV de 24 bits y lo añade** a la clave
4. El **emisor añade un identificador de clave** de 8 bits (Key ID)
5. Se introduce una clave de entrada (128 o 64 bits) con la que **se genera una clave de flujo**
6. Se **cifran los datos y el ICV** con RC4: [Bytes clave de flujo] XOR [Bytes datos + ICV]
7. **Se añade el identificador de clave y el vector de inicialización** al paquete (van en texto claro)
8. Se inserta la cara útil a una trama 802.11



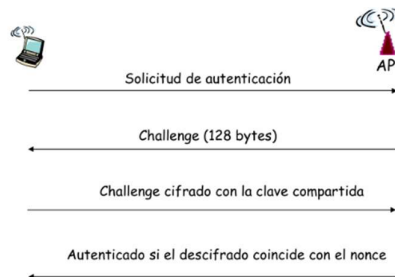
### Descifrado WEP

1. El receptor extrae el IV
2. Junto con la clave secreta compartida y el IV se introduce al generador pseudoaleatorio para dar la clave de flujo
3. Se hace una suma (XOR) de la clave de flujo con el contenido cifrado (datos + ICV) para descifrar el contenido
4. Se verifica la integridad de los datos con el ICV

## Autenticación de terminal

El sistema WEP se puede utilizar sin autenticación (Open) o con autenticación (Shared Key).

Cuando se usa el **modo de autenticación** el AP envía en su trama beacon que se necesita autenticación. Cuando un **dispositivo solicita conectarse el AP le envía un reto para que lo cifre con su clave y luego devolvérselo al AP. Una vez devuelto el AP comprueba si el cifrado ha sido el correcto y se lo comunica al dispositivo.**



## Rompiendo el cifrado WEP

En WEP existen muchos fallos que lo hacen inseguro:

- Usa una única clave secreta para todo (autenticación y confidencialidad) y la usan todos los dispositivos todo el tiempo
- La gestión de las claves es manual
- La autenticación solo es para el dispositivo cliente, la red o usuario no se autentican
- EL IV es muy pequeño y la forma en que se usa debilita aun más el protocolo

Entonces, los **principales agujeros de seguridad** son que el **IV es muy pequeño (24 bits)** y como se tiene que usar uno en cada trama al final se acabarán reutilizando y como se transmiten en texto plano, un atacante podría darse cuenta de que se están reutilizando.

Si se poseen los suficientes IVs se puede romper con relativa facilidad el cifrado WEP. Si no se tienen los suficientes la única opción es la fuerza bruta.

## ARP Request Replay Attack

El **ARP Request Replay Attack** tiene como objetivo **generar un gran volumen de tráfico para que finalmente los IV se terminen reutilizando.**

Este ataque se lleva a cabo mediante la **captura de paquetes ARP legítimos** y bien cifrados enviados por los clientes **para posteriormente volverlos a inyectar a la red y así generar tráfico** con los paquetes de respuesta. Los paquetes ARP se identifican porque tienen un tamaño muy reducido.

Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato  
→ Planes pro: más coins

pierdo espacio



Necesito concentración

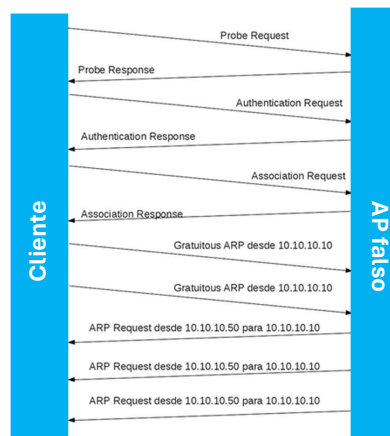
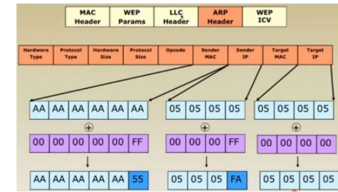
ali ali oohh  
esto con 1 coin me  
lo quito yo...

WUOLAH

## Caffe Latte Attack

El **Caffe Latte Attack** fue uno de los primeros ataques a aquellos equipos que no estaban conectados a un AP. El objetivo de este es mediante la **suplantación de un AP** hacer que un equipo se intente conectar a nosotros para crear tráfico y luego intentar descifrar la clave.

1. Aprovechando que los clientes se conectan de forma automática a los APs conocidos el atacante crea un **AP falso con el mismo SSID que el real**
2. La **victima recibirá un reto del AP y lo cifrará y se lo devolverá**
3. El **atacante dará por buena cualquier mensaje** de autenticación (el reto) que le llegue de vuelta
4. Tras realizar la "autenticación" el **cliente pide al AP mediante DHCP una IP** pero el AP nunca responderá
5. Tras un tiempo el **cliente se autoasignará una IP y comenzará a mandar Gratuitous ARP** indicando su IP, todo ello cifrado con la clave WEP
6. El AP utilizará una técnica que le permite **transformar ese Gratuitous ARP en un ARP Request** aplicando una transformación en unos bits en concreto (todo ello sin descifrar el Gratuitous ARP) y se crearán muchos paquetes con diferentes IP hasta dar con la que se autoasignó el cliente.
7. El **cliente responderá** a los ARP Request creando así más paquetes cifrados con WEP
8. Tras muchos paquetes se consiguen muchos IVs y el AP falso consigue crackear la clave



Si comparamos cuanto se tarda en llevar a cabo el ataque se aprecia que cuando se usa **WEP con autenticación se tarda mucho menos**, esto se debe a que se envían muchos más mensajes. Otra ventaja del uso de la autenticación WEP con este ataque es que al mandar un reto al cliente y devolvernos el cifrado del mensaje se pueden sacar 128 bytes de flujo de clave al tener el texto cifrado y claro, permitiendo enviar mensajes válidos de hasta 128 bytes.

Network Configuration	Approximate Cracking time
Shared + DHCP	~ 10 mins
Shared + Static IP	1.5 days
Open + DHCP	6 days
Open + Static IP	2 days

WUOLAH



## Korek's ChopChop Attack

El ataque **Korek's ChopChop Attack** se centra en el descifrado de un paquete, no de romper la clave de cifrado

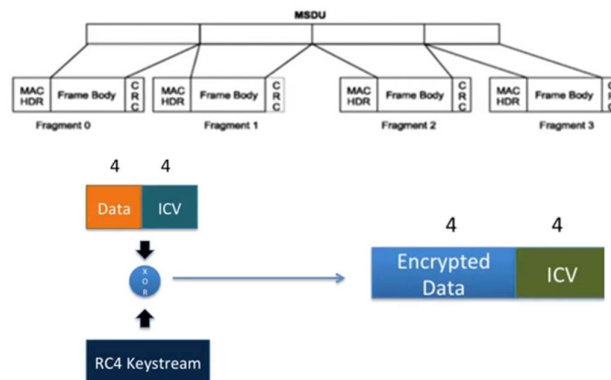
Este consiste en **modificar un paquete capturado** (cifrado con WEP) y quitarle el último **byte** de datos generando así un paquete más corto. A este nuevo paquete se va probando a **añadirle un nuevo último byte** y se **recalcula el ICV** hasta que el **AP lo acepta** y **entonces ya se conoce el último byte**. Este **proceso se repite** hasta descifrar el paquete completo.



## Fragmentation Attack




























En el **Fragmentation Attack** se **conoce el contenido** del LLC Header que es una **cabecera** que se pone al principio de los paquetes, por lo que **se puede conocer los primeros 8 bytes de flujo de clave RC4**. Al ser un flujo muy pequeño lo que se tendría que hacer es **segmentar un paquete de hasta 64 bytes en 16 subpaquetes de 8 bytes**.

Pero en realidad no se pueden cifrar 8 bytes por subpaquete, sino que **solo se puede incluir en cada uno 4 bytes de "carga util"**.

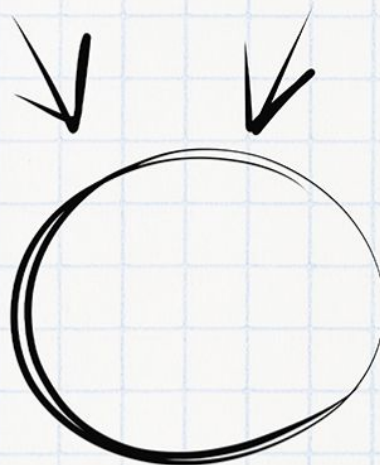


# Imagínate aprobando el examen

## Necesitas tiempo y concentración

Planes	 PLAN TURBO	 PLAN PRO	 PLAN PRO+
 Descargas sin publi al mes	10 	40 	80 
 Elimina el video entre descargas			
 Descarga carpetas			
 Descarga archivos grandes			
 Visualiza apuntes online sin publi			
 Elimina toda la publi web			
 Precios <span>Anual <input type="checkbox"/></span>	0,99 € / mes	3,99 € / mes	7,99 € / mes

Ahora que puedes conseguirlo,  
¿Qué nota vas a sacar?



# WUOLAH

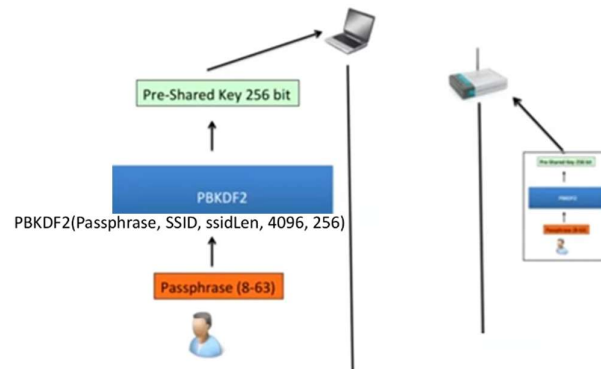
## CIFRADOS WPA Y WPA2 Y SUS ATAQUES

- **WPA:** se trata de una solución intermedia **basada en WEP**. Utiliza **autenticación con PSK** o 802.1X, emplea TKIP para **mejorar la seguridad de la clave** y **no requiere de cambios de hardware**.
- **WPA2:** es la solución que **se usa hoy en día**, emplea CCMP (**basado en AES**) y **requiere cambios de hardware** para soportarlo.

Ambas se pueden usar con la versión personal (con PSK [Pre Shared Key]) o Enterprise.

### WPA-PSK

**WPA-PSK** hace uso de una clave previamente compartida entre el cliente y el AP, la PSK. Esta clave no es con la que luego se cifrará todo el tráfico del cliente, sino que **con ella junto a más parámetros como el SSID se genera la clave (PBKDF2, Password Based Key Derivation Function) definitiva que cifrará las comunicaciones**.



### WIFI PROTECTED SETUP (WPS)

El **WPS** es un **estándar que facilita la configuración de equipos wifi en entornos domésticos**. Este se habilita mediante un botón en el router y evita tener que acceder a la configuración del router y tener que introducir la contraseña en router y dispositivo (sustituida normalmente por un pin de 8 dígitos). Es **altamente INSEGURA**.