

(in)Seguridad en redes WiFi

Diego Lendoiro : diego@inestable.org



(in)Seguridad en redes WiFi

- Introducción
 - Revisiones de 802.11
 - Topologías en redes WiFi.
 - Mecanismos de autenticación.
- Medidas de seguridad.
- Vulnerabilidades en WEP.
- Vulnerabilidades en WPA/PSK.
- Escenarios prácticos.



(in)Seguridad en redes WiFi

- Revisiones de 802.11
 - 802.11a
 - Banda espectral (ISM): 5Ghz
 - Modulación: OFDM
 - Tasa de transferencia: 54Mbps
 - Tipo de seguridad: WEP
 - Corto alcance



(in)Seguridad en redes WiFi

- Revisiones de 802.11
 - 802.11b
 - Ancho de banda espectral (ISM): 2.4Ghz
 - Modulación: DSSS
 - Tasa de transferencia: hasta 22 Mbps
 - Tipo de seguridad: WEP, WPA
 - Mejoras en el alcance → Disminución de costes



(in)Seguridad en redes WiFi

- Revisiones de 802.11
 - 802.11g
 - Banda espectral (ISM): 2.4Ghz
 - Modulación: DSSS y OFDM
 - Tasa de transferencia: hasta 54 Mbps
 - Tipo de seguridad: WEP, WPA (hasta 256 bits)
 - Mejoras en la tasa de transferencia debido a la modulación OFDM



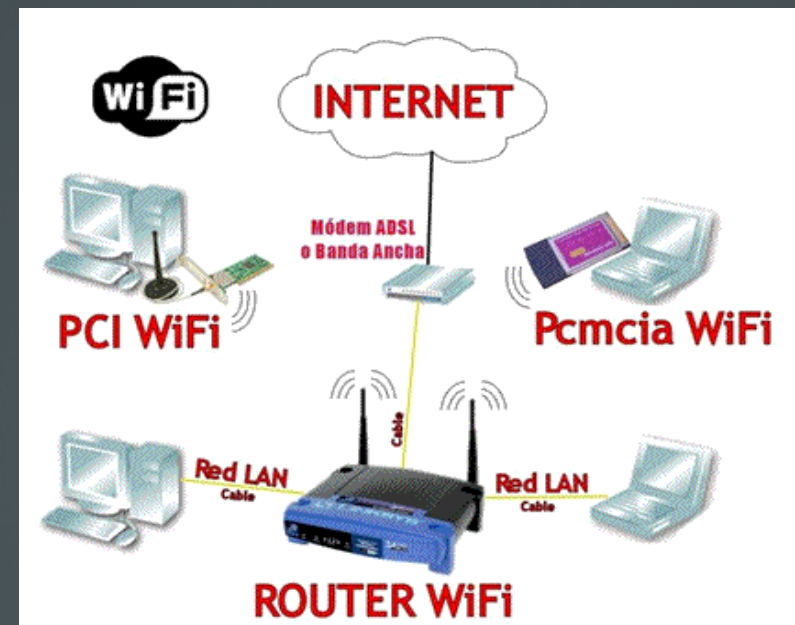
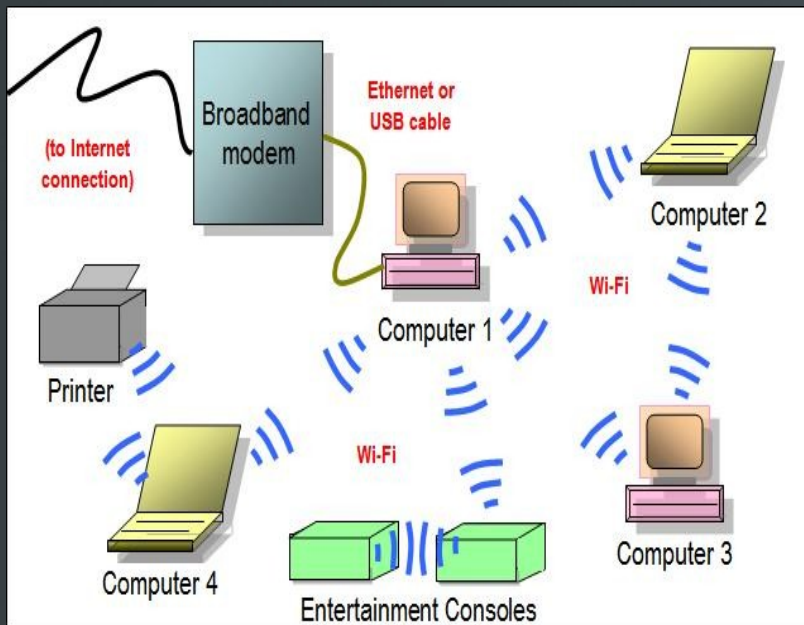
(in)Seguridad en redes WiFi

- Revisiones de 802.11
 - 802.11n
 - Banda espectral (ISM): 5Ghz
 - Tasas de transferencia: hasta 300Mbps
 - Modulación: OFDM
 - Tipo de seguridad: Según estándar 802.11i



(in)Seguridad en redes WiFi

- Topologías de red
 - Ad-hoc: Coordinación nula, cada estación se encarga de coordinarse a sí misma.
 - Infraestructura: Coordinación total mediante un nodo central (AP) que coordina a las STA.



(in)Seguridad en redes WiFi

- Mecanismos de autenticación
 - Open system: Cualquier estación es asociada a la red
 - Shared Key: Todas las estaciones han de conocer la passphrase para poder conectarse a la red.
- Proceso de autenticación shared key:

Cliente

AP

Authentication Request

Authentication Challenge

Authentication Response

Authentication Result

...



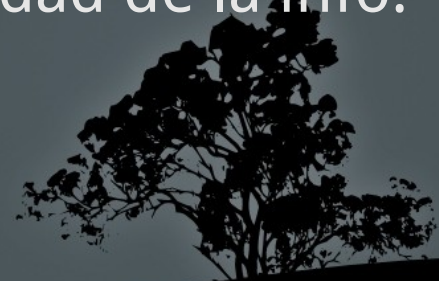
(in)Seguridad en redes WiFi

- Medidas de seguridad
 - ACL's : Listas de control de acceso basadas en las MAC's de las STA
 - SSID cloak: Ocultar el ssid en los beacon frames
 - WEP: Wired Equivalent Privacy
 - WPA: Wi-Fi Protected Access
 - Personal: Pre-Shared Key
 - Enterprise: Gestión de claves vía server RADIUS.



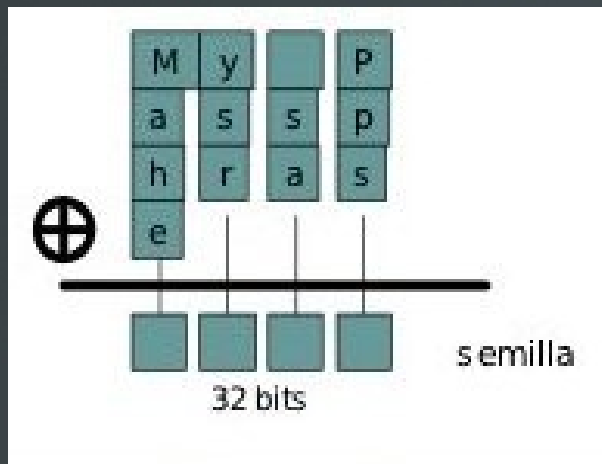
(in)Seguridad en redes WiFi

- WEP
 - Objetivo → Dar una seguridad equivalente al medio cableado en un medio cuyo acceso físico es más sencillo.
 - Cifrado de 64, 128 ó 256 bits (Realmente 40, 104 y 232)
 - Basado en RC4.
 - Las LLAVES que se utilizan para cifrar los datos se generan a partir de una PASSPHRASE que todas las estaciones deben conocer.
 - Uso de CRC para comprobar integridad de la info.



(in)Seguridad en redes WiFi

- WEP : Descripción del proceso de creación de la llave
 - Operación XOR entre los caracteres de la PASSPHRASE

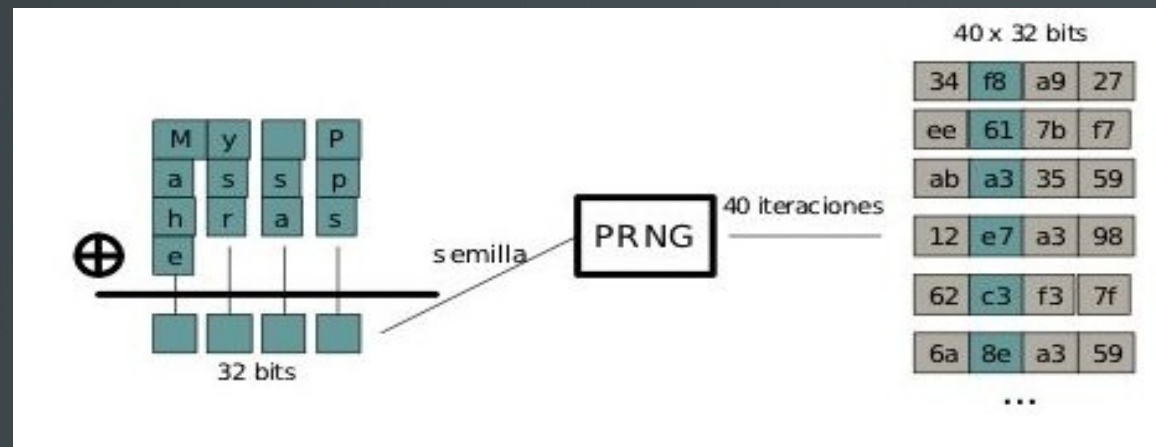


M=4d y=79 blank=20
a=61 s=73 P=50
h=68 r=72 p=70
e=65

4d XOR 61 XOR 68 XOR 65 = 21
79 XOR 73 XOR 72 = 78
20 XOR 73 XOR 61 = 32
50 XOR 70 XOR 73 = 53

(in)Seguridad en redes WiFi

- WEP: Descripción del proceso de creación de la llave
 - Una vez conseguida la semilla se utilizará el PRNG y se obtendrán 4 llaves (keys)



(in)Seguridad en redes WiFi

- WEP: Proceso de cifrado
 - Keystream: $RC4(\text{Vector inicialización}, \text{Key})$

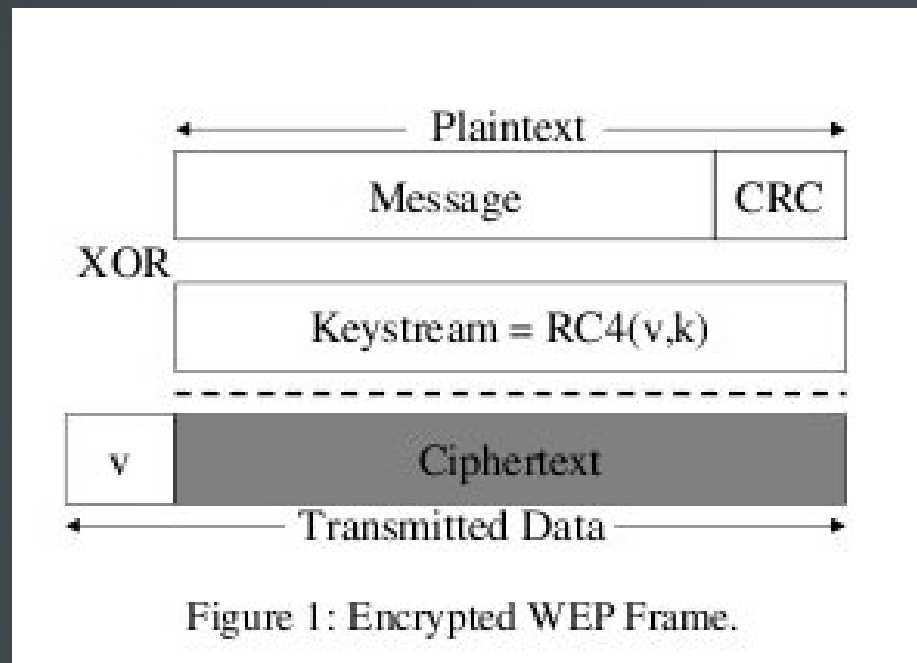


Figure 1: Encrypted WEP Frame.

(in)Seguridad en redes WiFi

- WEP: Problemas
 - IV 24 bits $\rightarrow 2^{24} = 16777216$ posibles IV diferentes
 - El IV es enviado sin ningún tipo de protección en las tramas de datos.
 - Reutilización de IV : Cualquier RTX implica un cambio de IV.
 - Índice secuencial : se puede predecir fácilmente
 - El keystream depende del IV.



(in)Seguridad en redes WiFi

- WEP: Vulnerabilidades y ataques
 - Vulnerabilidades en key scheduling (FMS attack)
 - Ataques de Korek
 - Ataque PTW
 - Ataque Chopchop



(in)Seguridad en redes WiFi

- WEP: Vulnerabilidades y ataques
 - FMS (Fluhrer, Mantin, Shamir) generalidades:
 - Paper publicado en 2001.
 - El IV se emplea para formar el keystream:
 $RC4(v,k)$.
 - Al enviarse sin cifrar nos permite conocer parte del keystream (3 bytes).
 - Estadísticamente podemos deducir la parte del keystream que pertenece a la llave.
 - Se requiere capturar gran cantidad de tráfico.



(in)Seguridad en redes WiFi

- WEP: Vulnerabilidades y ataques
 - Ataques de Korek:
 - Publicado en 2004.
 - Ataques estadísticos basados en FMS.
 - Reducción notable del número de paquetes necesarios para crackear el sistema.
 - Número de paquetes depende de método de generación del IV.
 - En torno a 300.000-500.000 paquetes



(in)Seguridad en redes WiFi

- WEP: Vulnerabilidades y ataques
 - Ataque PTW:
 - Publicado en 2007.
 - Mejora de los anteriores ataques estadísticos (FMS, Korek).
 - Menos condiciones a tener en cuenta para los paquetes → Reducción de paquetes necesarios
 - Mejora probabilística → Reducción de tiempo.
 - Alrededor de 24000 paquetes (!!).
 - Necesidad de paquetes ARP.
 - Método por defecto en suites como aircrack-ng



(in)Seguridad en redes WiFi

- WEP: Vulnerabilidades y ataques
 - Ataque chopchop y fragmentation:
 - No nos permiten recuperar la clave.
 - Permiten obtener PRGA para poder crear paquetes que el AP considere como válidos
 - Básicamente consiste en utilizar al AP como medio para obtener información sobre el PRGA.
 - "Si envío un 1 y el AP lo descarta entonces se que debería haber enviado un 0"



(in)Seguridad en redes WiFi

- Resumen:
 - WEP NO es seguro:
 - Con clientes asociados al AP.
 - Sin clientes asociados al AP.
 - Con ACL's basadas en MAC.
 - Ocultando el SSID.
 - Con cualquier combinación lineal de las anteriores.
 - ¿Cuales son las soluciones de las que disponemos?
 - WPA [Personal/Enterprise]
 - WPA2 [Personal/Enterprise]



(in)Seguridad en redes WiFi

- WPA Personal (PSK):
 - WiFi Protected Access características:
 - Diseñado para funcionar en las tarjetas antiguas
 - Mejora de WEP gracias a TKIP
 - Temporary Key Integrity Protocol
 - Continúa utilizando RC4 para el cifrado del IV
 - Cambio de claves cada 10000 paquetes
 - Implementación de MIC (soluciona problemas de CRC)
 - Inclusión de un TSC para impedir ataques de inyección




(in)Seguridad en redes WiFi

- WPA Problemas conocidos:
 - En entornos WPA/WPA2 Personal con clave compartida
 - Ataques por fuerza bruta capturando handshake
 - Dependiendo de la longitud de la clave podría llevarnos de unas horas a varios días.
 - Consumo de CPU elevadísimo.
 - Uso de la GPU (Graphics Process Unit) con pyrit:
 - <http://code.google.com/p/pyrit/>
 - Reducción del tiempo de proceso.



(in)Seguridad en redes WiFi

- WPA Problemas conocidos:
 - Cracking por bruteforce → Demasiado costoso
 - En 2008 se publica el primer documento en el cual se explica como saltarse el proceso de chequeo de integridad de WPA (MIC)
 - Aparece como consecuencia de ser un sistema heredado de WEP (Similar a un ataque chopchop)
 - No permite obtención de clave pero si inyección de tráfico.
 - Se basa en tramas ARP.
 - Sistemas WPA-PSK (TKIP) quedaban en entredicho aunque no vulnerados (Ataques Beck-Tews)
- 

(in)Seguridad en redes WiFi

- WPA Problemas conocidos:
 - A finales de 2009 se publica otro paper que describe una nueva vulnerabilidad.
 - Es un avance respecto de los ataques Beck-Tews.
 - Hace uso de ataques MITM.
 - Un atacante podría capturar el tráfico de los clientes.
 - A diferencia de los ataques Beck-Tews no necesita que la red tenga QoS habilitado.
 - No se ha liberado una implementación del ataque todavía.
 - No tiene efecto sobre WPA2.



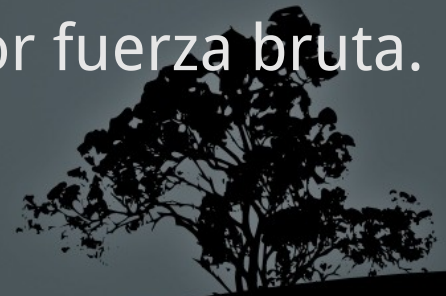
(in)Seguridad en redes WiFi

- WPA resumen:
 - WPA en sus versiones Pre Shared Key tiene deficiencias
 - A día de hoy no se puede considerar seguro a la espera después de los últimos papers liberados.
 - Sin embargo sigue siendo empleado debido a la gran proliferación de tarjetas wifi antiguas.
 - Sigue siendo una mejor opción que WEP.



(in)Seguridad en redes WiFi

- ¿Qué método sería el correcto para la red de nuestra casa?
 - WPA2 Personal
 - Es la mejor opción, nos curaremos en salud.
 - No necesita desplegar servidores RADIUS. → inviable en una red casera.
 - Usa cifrado AES y CCMP
 - Problemas:
 - Soporte por parte de la infraestructura.
 - Susceptible a ciertos ataques DoS % muy bajo.
 - Sigue pudiéndose romper por fuerza bruta.



(in)Seguridad en redes WiFi

- ¿Preguntas?



(in)Seguridad en redes WiFi

- Estas transparencias no serían posibles sin las presentaciones de: Pablo Garaizar, Ricardo Galli, PoF y muchos otros.
- Además por supuesto de los papers oficiales de Beck - Tews, Toshihiro – Morii
- Y la inestimable ayuda de los sitios de referencia en estos temas: aircrack-ng.org, remote-exploit.org
- Ah! Y gracias a la enciclopedia de bolsillo: wikipedia.org

