Técnicas avanzadas de ataque en redes inalámbricas

Raúl Siles, GSE, Hewlett-Packard
David Pérez, GSE, Consultor independiente

Red IRIS

Ponentes

- **Raúl Siles**

  Consultor de seguridad, HP

  GSE

  raul@raulsiles.com

- **David Pérez Conde**

  Consultor independiente de seguridad

  GSE

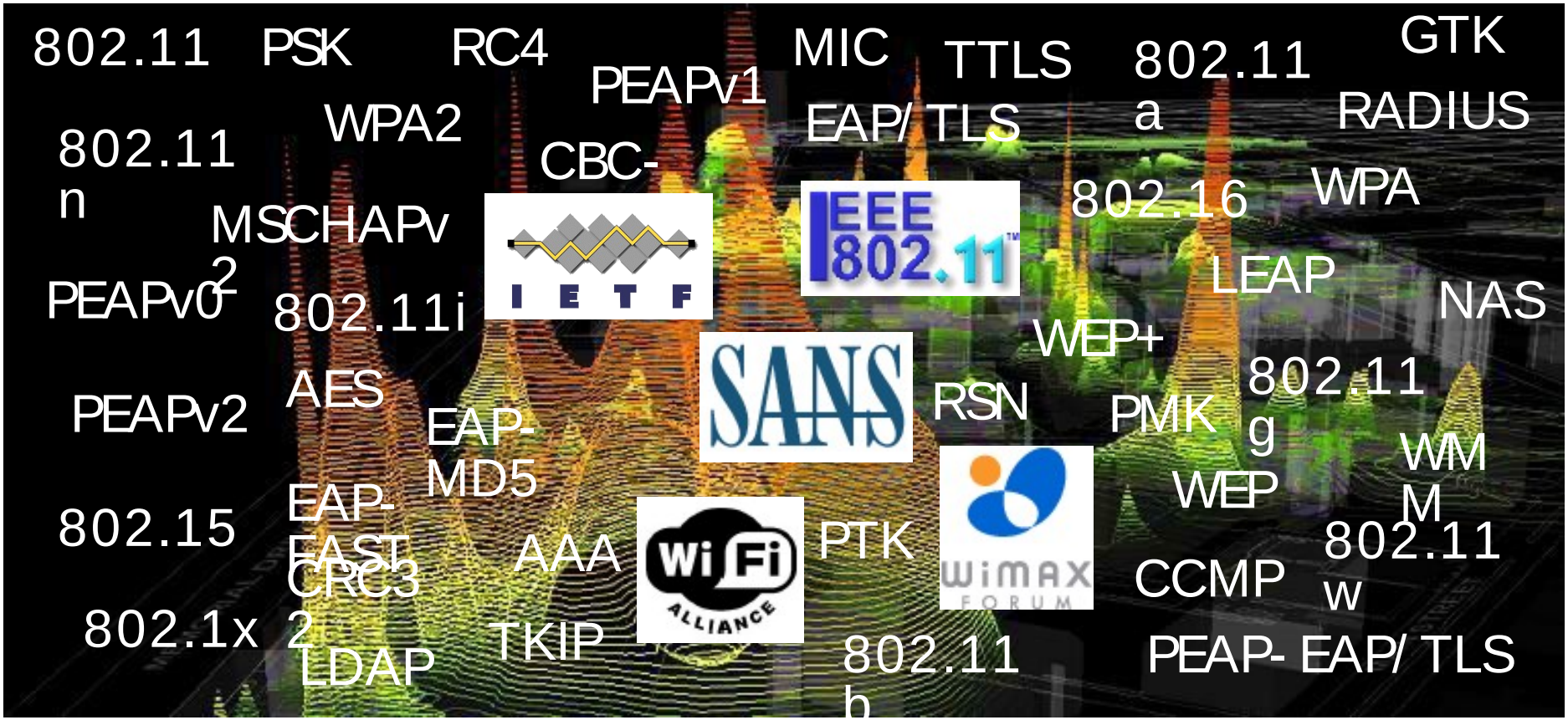
  david.perez.conde@gmail.com

Agenda

- ¿(In)seguridad en redes inalámbricas 802.11_ (WiFi)?
- Historia de la seguridad WiFi:
  - Interceptación de tráfico, identificación de la red, cambio de MAC, obtención de la clave WEP, retransmisión de tráfico, inyección de tráfico, ataque inductivo inverso, MITM, ataque de diccionario (WPA-PSK), Denegación de Servicio (DoS)
- Recomendaciones de seguridad en redes WiFi
- Referencias

¿(In)seguridad WiFi?

- *¿Cuál es el estado actual de la (in)seguridad WiFi?*

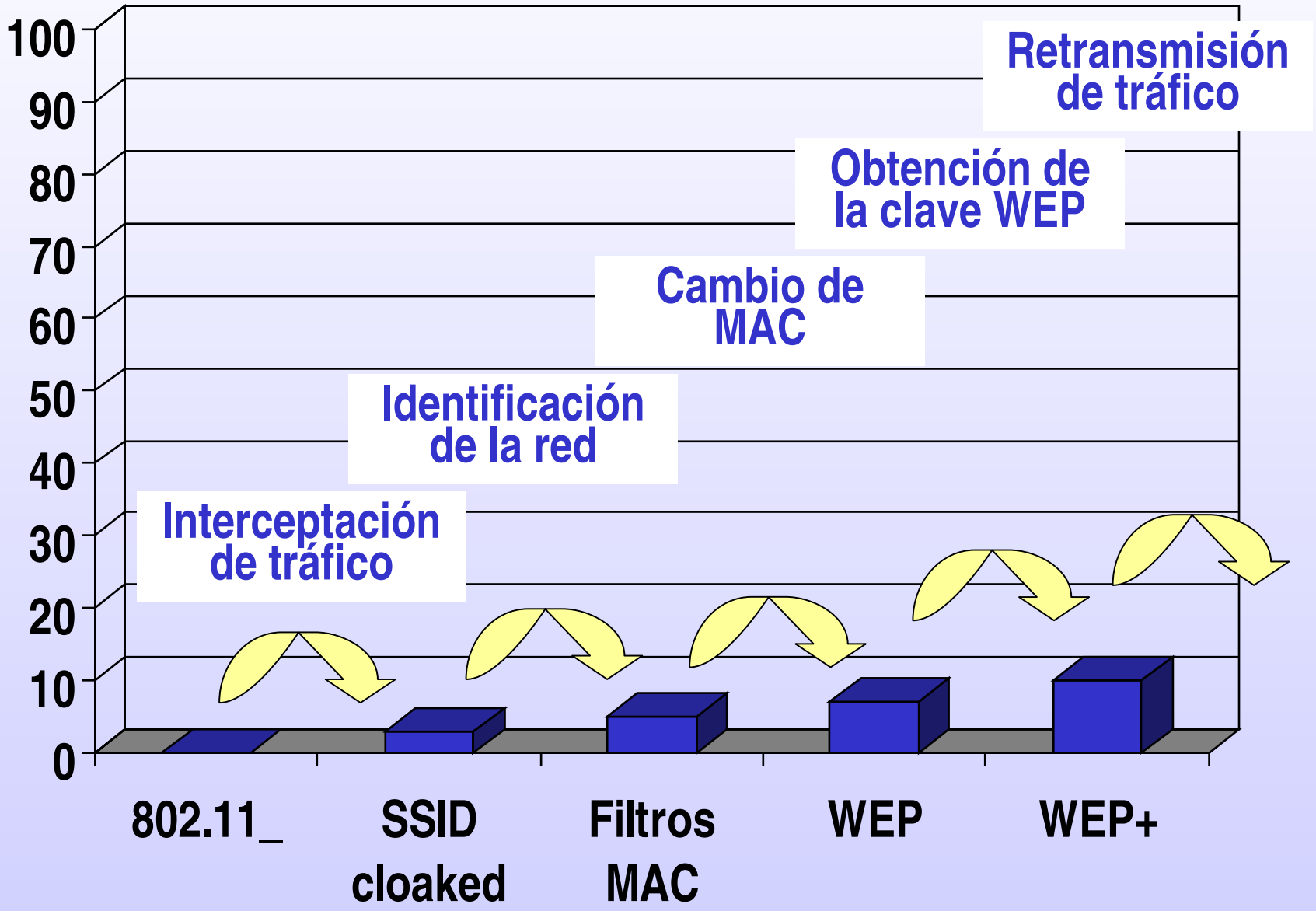


IV Foro de Seguridad de RedIRIS

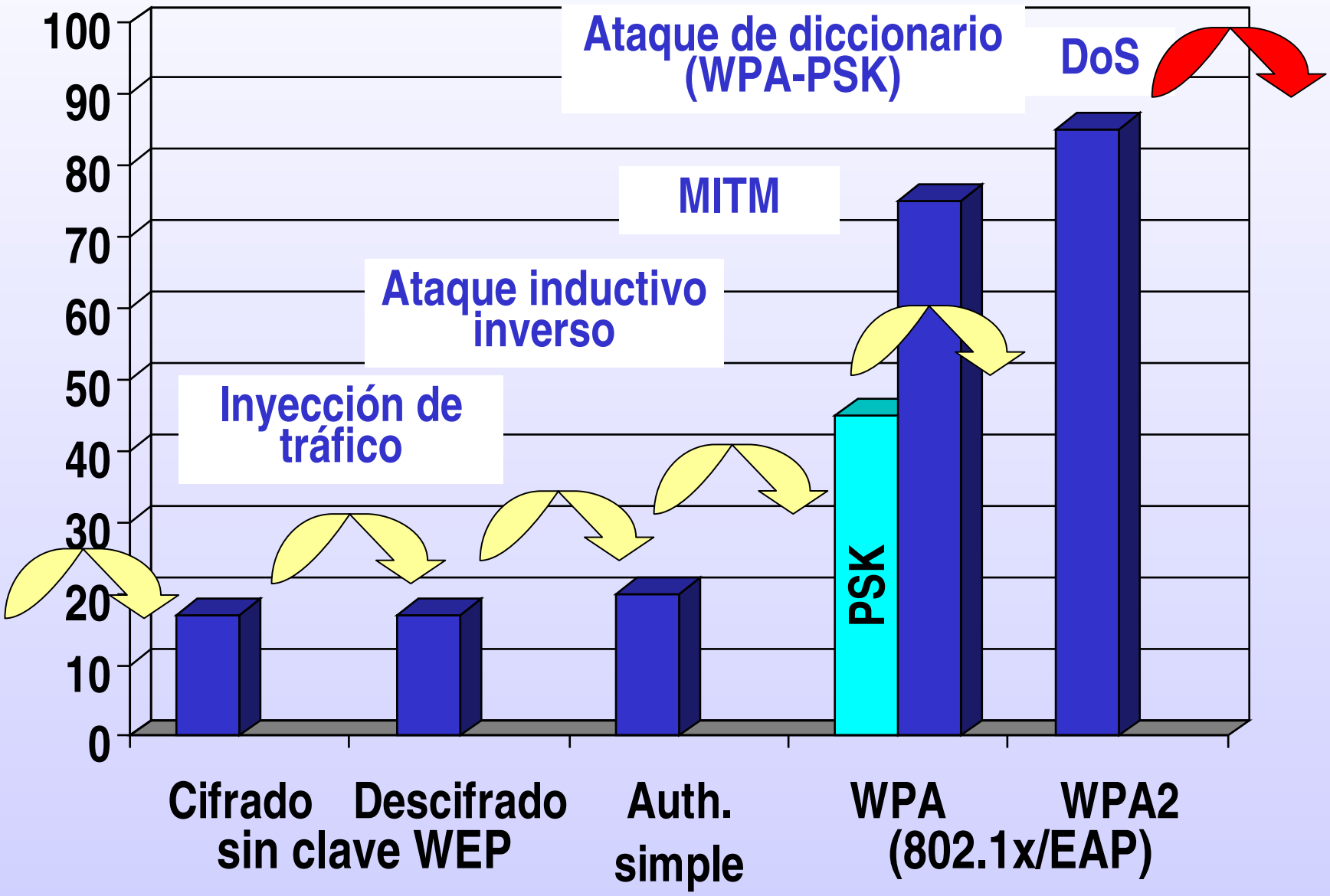
Técnicas avanzadas de ataque en redes inalámbricas

hp invent

Historia de la seguridad WiFi



Historia de la seguridad WiFi (2)



Interceptación de tráfico

- ¿Medio físico? ¿Seguridad física?
- Medio compartido HUB.
- Captura de tráfico: pasiva e indetectable.
- Modo monitor (RFMON) vs Modo promíscuo.
- Tramas: datos, gestión y control.
- Calidad de la señal: asociación vs interceptación.
- GPS, antenas, ¿WiMAX? …
- *¿Cuál es la máxima distancia requerida para establecer una conexión 802.11b?*
- Auditor CD, cliente vs RFMON, ethereal.

Defcon WiFi Shootout 2005 (802.11b)

Identificación de la red (SSID)

- El SSID es el identificador o nombre de la red.
- **NO** es una clave de acceso.
- Los valores por defecto de los distintos fabricantes son conocidos.
- El punto de acceso (AP) lo anuncia públicamente de forma continua (*SSID broadcast*).
- Es posible desactivar su propagación convirtiendo la red en encubierta (*cloaked network*).
- *¿Puede obtenerse en este caso?*
- Netstumbler (Win) vs kismet (Linux).

Cambio de dirección MAC

- Restringir el acceso a la red a un conjunto de direcciones físicas (MAC) válidas.
- La MAC es única para cada tarjeta de red.
- La MAC se transmite en claro en cada trama.
- Resulta inmanejable para grandes entornos.
- *¿Es posible tener acceso?*
- La MAC puede cambiarse mediante software.
  Ejemplo: ifconfig (Linux) o SimpleMAC (Win).
- Paciencia vs ¿Duplicación de dirección MAC?

Obtención de la clave WEP

- WEP es **W**ired **E**quivalent **P**rivacy.
- Mecanismos de seguridad:
  - Cifrado: RC4, cifrador de flujo (XOR).
  - *Claves*: 64, 128, 256 bits.
  - IV: 24 bits de vector de inicialización
  - Clave = secreto + IV 40, 104, 232 bits.
  - IV transmitido en cada trama en claro (secuencial).
  - Autentificación mediante la misma clave de cifrado (WEP).
  - Integridad (ICV) usando CRC-32.
- PRGA = RC4(Clave, longitud datos)

Obtención de la clave WEP (2)

- Texto claro ⊕ PRGA = Texto cifrado.
- Existen IVs débiles que permiten recuperar posiciones de la clave WEP.
- Ataque FMS: Fluhrer, Mantin and Shamir.
- La clave es común a toda la red y no se dispone de mecanismos de rotación de claves.
- La obtención de la clave WEP permite conexión a la red y descifrar los datos.
- *¿Es posible obtener la clave completa?*
- Airodump y aircrack.

Retransmisión de tráfico

- Es necesario un número suficiente de IVs para derivar la clave.
- *¿Qué ocurre si no hay tráfico en la red?*
- Es posible retransmitir paquetes capturados previamente sin modificar.
- Las respuestas al tráfico retransmitido proporcionan nuevos IVs débiles.
- No existe protección frente a retransmisiones ni existe el concepto de tramas secuenciales.
- WEP+ elimina los IVs débiles identificados inicialmente (9000). Nuevos ataques estadísticos sobre los IVs. (5,5M).
- Aireplay.

Inyección de tráfico sin la clave

- *¿Es posible inyectar tráfico cifrado en la red sin conocer la clave WEP?*
- Autentificación:
  - Abierta: siempre se permite el acceso.
  - Cerrada: *challenge/response* con la clave WEP.
- *¿Cuál es mejor en el caso de WEP?*
- Autentificación WEP: *challenge/response* de 128 bytes de texto claro y cifrado.
- Texto claro ⊕ Texto cifrado = PRGA.
- Mecanismo de autentificación débil que permite derivar PRGA.

Inyección de tráfico sin la clave (2)

- *¿Qué se puede hacer con la PRGA?*
- Inyección de cualquier paquete cifrado del tamaño de la PRGA.
- También es posible identificar tráfico en base a la longitud y a las cabeceras del paquete.
- Es posible obtener PRGA > 128 bytes.
- Texto Cifrado = Texto Claro ⊕ PRGA.
- WEPWedgie.

Ataque inductivo inverso

- *¿Es posible descifrar tráfico sin conocer la clave WEP?*
- Verificación de integridad mediante ICV (CRC-32).
- Descifrado byte a byte.
- Eliminar el último byte del texto cifrado (C-1): inválido.
- C-1 ⊕ 0…255: válido.
- Proporciona el texto en claro y, por tanto, la PRGA.
- ¡¡Gracias, punto de acceso!!
- Chopchop.

MITM

- Interceptación y modificación del tráfico situándose entre los clientes y el AP.
- Suplantación del AP mediante técnicas de la capa 1 (RF/señal) y de la capa 2 (MAC/802.11):
  - Mismo SSID.
  - Mejor señal y menos ruido.
- Vulnerabilidades:
  - Autentificación básica: El cliente se valida frente al AP.
  - Falsificación de direcciones (*MAC spoofing*).
- Autentificación mútua robusta entre cliente **y** AP.
- Hotspotter.

Ataque de diccionario (WPA-PSK)

- WPA es **W**i-Fi **P**rotected **A**ccess.
- Se diseñó para reemplazar temporalmente al fracasado WEP antes de disponer de 802.11i (WPA2).
- Proporciona compatibilidad con el hardware existente y permite actualizaciones mediante software.
- Define múltiples claves: PSK (compartida), PMK (maestra), PTK (temporales)…
- WPA-Personal (clave compartida, PSK) o WPA-Empresarial (RADIUS,802.1x/EAP).
- *¿Es WPA vulnerable?*
- Cowpatty.

Denegación de Servicio (DoS)

- Saturación del medio físico (RF, Radio Frecuencia).
- Debilidades en los protocolos 802.11:
  - Inundación de tramas de desautentificación/desasociación.
  - Inundación de tramas de autentificación/asociación.
- Ataques sobre los clientes/APs: vulnerabilidades hw y sw.
- Complemento para realizar otros ataques: MITM.
- Duración limitada o permanente.

¡¡ La gran debilidad de WiFi !!

Denegación de Servicio (DoS) (2)

- DoS en el diseño de WPA y WAP2 (802.11i).
- Integridad WPA: Michael (29 bits de seguridad).
- Limitado por la potencia de cálculo del hardware objetivo.
- Fuerza bruta: 2^{29}. 11Mbps (50%): 2 minutos.
- Contramedidas: Si el AP recibe 2 paquetes con un MIC inválido en 60 segundos, la especificación 802.11i requiere que el AP desautentifique a todos los usuarios y se apague durante 60 segundos. Al volver a activarse se deben renovar todas las claves.
- *¿Real?* Deben superarse otras medidas, como el control de nº. de secuencia y el chequeo CRC32 (ICV).
- WMM (Wireless MultiMedia)…

Recomendaciones de seguridad en redes WiFi

- Defensa en profundidad WiFi:

  SSID, filtrado de direcciones MAC…
- Cifrado e integridad:
  - WPA-Personal (PSK +20 caracteres).
  - WPA/WPA2-Enterprise.

WPA-PSK (*Passphrase*):

PSK: 8-63 chars = 63 + ”\0” PMK = 256 bits (64 HEX)

http://www.grc.com/pass

Recomendaciones de seguridad en redes WiFi (2)

- Autentificación:
  - 802.1X/EAP: múltiples tipos.
  - Autentificación mutua para evitar MITM (Ej.- PEAP, EAP-TLS, TTLS…).
  - Certificados de cliente y de servidor (Ej.- EAP-TLS).
- DoS:
  - Capa física: alcance de la señal.
  - 802.11 MAC: 802.11w (2007).
- WIDS.

Recomendaciones de seguridad en redes WiFi (3)

- Defensa en profundidad general:
  - Securización de los clientes, puntos de acceso, servidores RADIUS, switches…
  - Logging (Ej.- Syslog).
- Monitorización:
  - Utilización: acceso de usuarios y tráfico.
  - Nivel de señal (RF) y redes inalámbricas (*Rogues*).
  - Gestión de cambios: configuración de los puntos de acceso y versiones de software.
- Políticas de uso e instalación de redes inalámbricas.

¡¡Muchas gracias!!

Referencias

ESTÁNDARES:

- IEEE 802.11. http://grouper.ieee.org/groups/802/11/
- Wi-Fi Alliance. http://www.wi-fi.org
- IETF: http://www.ietf.org/

ARTÍCULOS:

- Weaknesses in the Key Scheduling Algorithm of RC4. S. Fluhrer1, I. Mantin2, & A. Shamir. Aug, 2001. http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf.
- (In)Security of the WEP algorithm. N. Borisov, I. Goldberg & D. Wagner. 2001.http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- Cracking WEP. Seth Fogie. July 12, 2002. http://www.samspublishing.com/articles/printerfriendly.asp?p=27666&rl=1

Referencias (2)

ARTÍCULOS (cont.):

- Cracking Wi-Fi Protected Access (WPA), Part 1. Seth Fogie. March 4, 2005. http://www.informit.com/articles/printerfriendly.asp?p=369221
- Cracking Wi-Fi Protected Access (WPA), Part 2. Seth Fogie. March 11, 2005. http://www.informit.com/articles/printerfriendly.asp?p=370636
- Four Ways To Monitor Your Wireless Network SANS Webcast. October, 2005. https://www.sans.org/webcasts/show.php?webcastid=90561
- Migrating from WEP to WPA2. SANS Webcast January, 2006. https://www.sans.org/webcasts/show.php?webcastid=90559

FORMACIÓN:

- SANS "SECURITY 617: Assessing and Securing Wireless Networks". http://www.sans.org

Más referencias:

- http://www.raulsiles.com/resources/wifi.html

Referencias (3)

HERRAMIENTAS:

- Auditor CD. http://new.remote-exploit.org/index.php/Auditor_main
- BackTrack. http://www.remote-exploit.org/index.php/BackTrack
- Ethereal. http://www.ethereal.com
- Netstumbler. http://www.netstumbler.com
- Kismet. http://www.kismetwireless.net
- SimpleMAC. http://dukelupus.pri.ee/simplemac.php
- Aircrack (incluyle aireplay, airodump). http://freshmeat.net/projects/aircrack
- WEPWedgie. http://sourceforge.net/projects/wepwedgie
- Chopchop. http://www.netstumbler.org/showthread.php?t=12489
- Hotspotter. http://www.remote-exploit.org/index.php/Hotspotter