RIESGOS DE LAS REDES INALÁMBRICAS

Las redes inalámbricas Wi-Fi han posibilitado la sustitución de los cables por ondas de radio. De este modo, se eliminan las ataduras y limitaciones de los dispositivos de conexión. Pero también permiten una mayor facilidad para que cualquiera tenga acceso a los datos que circulan por la red. Si con los cables un atacante debía obtener acceso físico a un punto de acceso para poder realizar alguna acción, con las redes inalámbricas esta tarea se vuelve trivial. Al eliminarse el componente físico que podía llegar a proteger los datos, éstos quedan mucho más expuestos.

Por tanto, si se quiere hacer un uso responsable y seguro de esta tecnología, el modelo de redes inalámbricas debe centrarse en el cifrado de los datos. A continuación se exponen los riesgos a los qué están expuestas estas redes y las recomendaciones generales para evitarlos.

I Terminología previa

Existe una gran cantidad de terminología acerca de las redes inalámbricas que no siempre es correctamente entendida. Se diferencia cada una de ellas con una breve descripción.

a. **Estándar IEEE 802.11**: define específicamente el uso de los dos niveles inferiores de la arquitectura OSI (capa física y de enlace de datos), detallando las normas de funcionamiento en una WLAN a esos niveles. Deben seguirlo todos los fabricantes de dispositivos que soporten esta tecnología para que puedan entenderse entre ellos. Cuando se incorpora una variación, se añade una letra. Así IEEE 802.11n, por ejemplo, es de los más usados. IEEE 802.11i llega a los 600 Mbps en capa física. 802.11i se definió específicamente para mejorar la seguridad. IEEE 802.11b, IEEE 802.11g e IEEE 802.11n son aceptados internacionalmente porque la banda de 2.4 GHz está disponible de forma casi universal. Estos estándares son conocidos luego por el gran público bajo nombres mucho más asequibles como WPA o WPA2.

b. **Wi-Fi**: es una marca perteneciente a la Wi-Fi Alliance (agrupación de marcas comerciales como Nokia, Microsoft, Apple, Belkin, etc). Estas se encargan de certificar que los dispositivos cumplen el estándar IEEE 802.11 y que, por tanto, pueden operar con otros compatibles. Wi-Fi y su logo de ying y el yang, no son más que una forma de la industria de certificar que el producto que lo posee, cumple el estándar.

Ilustración 1: Logotipo comercial de la Wi-Fi Alliance

Fuente: www.wi-fi.org

c. **WEP**: acrónimo de *Wired Equivalent Privacy* es el primer sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes inalámbricas que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2 del modelo OSI. Utiliza el algoritmo criptográfico RC4 para cifrar y CRC-32 para la integridad. En el sistema WEP se pueden utilizar dos métodos de autenticación: Sistema abierto y clave compartida.

   El problema con WEP no está en RC4, sino en cómo lo implementa. WEP no crea bien el vector de iniciación del algoritmo, y hace que los vectores sean predecibles para incrementar el vector de un paquete a otro. Además existe un problema con el tamaño de los vectores de iniciación. Todo esto ha hecho que WEP se considere inseguro, y que existan numerosas herramientas capaces de averiguar en cuestión de minutos la clave con la que están cifrados los datos. Para limitar estos ataques, se creó WEP+.

d. **WPA**: WPA implementa la mayoría del estándar IEEE 802.11i y fue creado por Wi-Fi Alliance para corregir WEP de forma transitoria. Se necesitaba algo que corrigiera WEP, pero que a su vez fuese compatible con el hardware del momento. Mientras se esperaba a que estuviese preparado y definido WPA2, la alianza creó un sistema intermedio. WPA fue diseñado para utilizar un servidor de autenticación (normalmente Radius), que distribuye claves diferentes a cada usuario. También se puede utilizar en modo de clave pre-compartida (PSK, *Pre-Shared Key*), menos seguro que con el servidor Radius.

   La información es cifrada utilizando el algoritmo RC4 (porque debía ser compatible con lo ya existente) pero mejorado y bien implementado. La clave es de 128 bits y el vector de inicialización de 48 bits. Una de las

mejoras fundamentales sobre WEP es la implementación del Protocolo de Integridad de Clave Temporal (TKIP o *Temporal Key Integrity Protocol*), que cambia claves dinámicamente a medida que el sistema es utilizado. Fue específicamente diseñado, junto con un vector de inicialización (IV) mucho más grande, para evitar los ataques ya conocidos contra WEP.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información. Con CRC era posible alterar la información y actualizar la CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad mejorado (MIC o *Message Integrity Code*), también conocido como *Michael*. Además, WPA previene contra ataques de repetición, puesto que incluye un contador de tramas.

e. **WPA2**: es de nuevo, una certificación, pero no obliga al dispositivo al uso de ninguna de tecnologías de cifrado específica. Un dispositivo certificado WPA2 puede utilizar tanto el algoritmo de cifrado AES, (mucho más seguro y robusto) como RC4 (y por tanto, el protocolo TKIP). Cuando un dispositivo que soporta WPA2 usa el algoritmo de cifrado AES, lo hace dentro del protocolo CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) que es más seguro que TKIP. En la mayoría de dispositivos la denominación es utilizada erróneamente, y se habla de TKIP o AES, cuando en realidad se debería decir TKIP o CCMP. La confusión procede de que el protocolo CCMP utiliza el algoritmo de cifrado AES.

f. **Redes**: una red inalámbrica tiene dos componentes principales: las estaciones (STA) y los puntos de acceso (AP). Pueden operar en dos modalidades: 1) en ad-hoc, en la que cada cliente (STA) se comunica directamente con los otros clientes de la red y 2) en infraestructura, donde las STA envían los paquetes a una estación central llamada punto de acceso.

Tabla 1: Comparativa tecnologías de cifrado Wireless

Tecnología	Integridad	Cifrado	Autenticación	Protocolo
WEP	CRC-32 *Cyclic redundancy check*	RC4 (Mal implementado)	Sistema abierto o clave compartida	
WPA	MIC o Michael *Message authentication code*	RC4	PSK (*Pre-shared key*) Radius	TKIP *Temporal Key Integrity Protocol*
WPA2	AES *Advanced Encryption Standard*	AES *Advanced Encryption Standard*	PSK (*Pre-shared key*) Radius	CCMP *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*

Fuente: INTECO

II Recomendaciones de seguridad en las comunicaciones inalámbricas

La seguridad de las comunicaciones inalámbricas se basa principalmente en tres funciones:

a. Cifrar de forma eficaz la comunicación, para lo cual se debe usar WPA2 con Radius.

b. Limitar el acceso, estableciendo un control de acceso eficaz.

c. Proteger con contraseñas seguras y robustas con más de 30 caracteres, que combinen números, letras, símbolos, mayúsculas y minúsculas.

Una vez se dispone del conocimiento de la tecnología disponible para alcanzar estos objetivos, las recomendaciones son las siguientes:

- Filtrado de direcciones MAC.
- Uso de WPA2 bien configurado.
- Ocultación de SSID.
- Evitar el uso de DHCP.
- Diseño de red.

Los siguientes apartados profundizan en cada una de estas recomendaciones.

Filtrado de direcciones MAC

Los puntos de acceso deben tener una relación de las direcciones MAC que pueden conectarse a ellos.

La dirección MAC (*Media Access Control*) es un identificador único que se asigna a todas y cada una de las tarjetas de red existentes y que se graba en ellas en una memoria especial. Lo hace el propio fabricante de la tarjeta o dispositivo, y consiste en una serie de números que identifican unívocamente a esa tarjeta de red. De esta secuencia de números se pueden deducir una serie de datos como por ejemplo el fabricante (marca de la tarjeta). También es conocida como la dirección física o dirección hardware.

No es un método que ofrezca un alto grado de seguridad, puesto que un atacante puede falsear su dirección y hacer que coincida con una de las permitidas, pero es una medida básica para evitar que cualquiera pueda acceder a la red de forma trivial. Para conocer cuáles son las direcciones MAC permitidas, el atacante solo tiene que obtener algún tráfico de red, puesto que esta dirección, por definición y obligatoriamente, viaja sin cifrar en cada paquete de información que se transmite.

Uso de WPA2 bien configurado

WPA2 es la certificación más robusta que se conoce para Wi-Fi hasta el momento. Es importante que se utilicen, dentro de ella, las tecnologías adecuadas para proteger la información. En este momento esto se consigue con el Protocolo CCMP, que incluye el cifrado AES, puesto que en TKIP se han encontrado ya ciertos problemas de seguridad.

Otra medida básica es utilizar contraseñas largas, robustas, complejas y que estén almacenadas en un lugar seguro. Si no posible utilizar un servidor Radius, se puede utilizar PSK (clave previamente compartida). La ventaja de utilizar un servidor estándar Radius es que, en este caso, cada usuario contará con una contraseña, en vez compartir una misma contraseña entre todos los que se conecten con el punto de acceso. Así, si una clave de usuario quedase comprometida, el atacante solo tendría acceso a la información transmitida entre ese usuario y el punto de acceso.

Ocultación del SSID

El SSID (*Service Set Identifier*) es una cadena usada por los nodos de acceso de redes inalámbricas por el que los clientes son capaces de iniciar conexiones. Es necesario elegir un SSID único y difícil de adivinar en cada punto de acceso y, si es posible, que no se publique, de forma que los usuarios que lo necesiten deban introducir este valor de forma manual a la hora de encontrar la red inalámbrica.

Al igual que ocurre con el filtrado MAC, un atacante podría llegar a descubrir el SSID aunque no esté publicado.

Evitar el uso de DHCP

El protocolo DHCP consiste en el reparto automático de direcciones IP por parte del servidor central si el cliente no posee una dirección fija. Esto facilita un potencial ataque puesto que si el intruso logra entrar en la red, no debe preocuparse por utilizar una IP que ya esté en uso ni por el rango válido que acepte el servidor, sino que ésta se le ofrece automáticamente.

Si se utiliza DHCP, se debe limitar el número de direcciones disponibles. Así, en la medida de lo posible, no deben quedar direcciones libres en el rango que potencialmente puedan ser utilizadas por un atacante.

No usar DHCP no es una medida que proteja de forma absoluta, pero sí contribuye a una implementación de una red más segura por capas.

Diseño de red

Es de las medidas más importantes a adoptar. Como paso previo a la aplicación de medidas de protección de una red inalámbrica, es importante diseñar la red de forma correcta. Algunas medidas básicas a implementar son (también válidas para las redes físicas):

- Establecer redes privadas virtuales (VPN) a nivel de cortafuegos, para el cifrado adicional del tráfico de la red inalámbrica.
- No deben conectarse directamente los puntos de acceso a la red interna de una empresa. Las redes inalámbricas deben recibir el mismo trato que cualquier otra red insegura, como puede ser la conexión a Internet. Por tanto, entre la red inalámbrica y la red interna deberá existir un cortafuegos y, además, mecanismos de autenticación.
- Los clientes de las redes inalámbricas deben acceder a la red utilizando mecanismos tales como *Secure Shell* (SSH), redes privadas virtuales (VPN) o IPSec. Estos mecanismos facilitan los mínimos necesarios en lo referente a la a autorización, autenticación y cifrado del tráfico.

III Ataques actuales contra redes Wireless

Existen ataques conocidos contra las redes que se han ido desarrollando con los años. Conocerlos es necesario para poder protegerse frente a ellos.

Evil twin Networks

Evil Twin es un término usado para lo que podría ser denominado como "secuestro" de la conexión por redes inalámbricas ilegítimas. El peligro se centra en el usuario de redes inalámbricas, más que en las redes en sí.

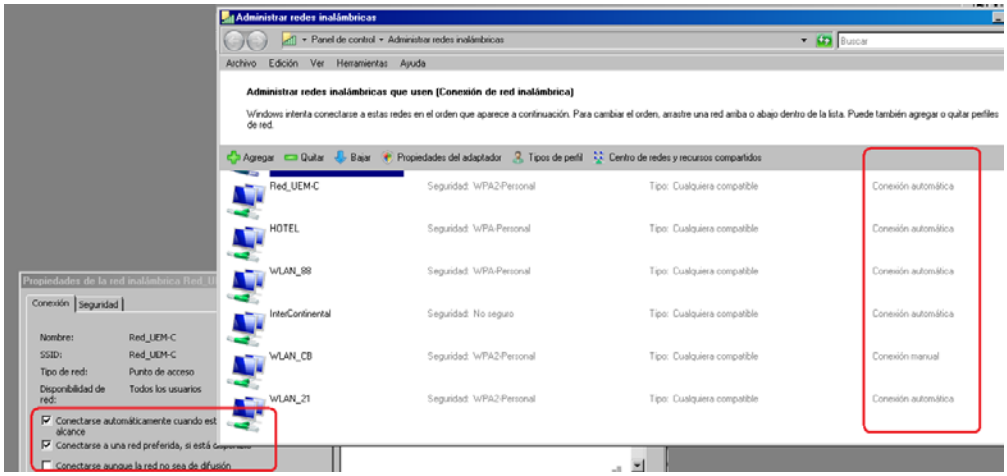
Con la popularidad de las redes inalámbricas disponibles en puntos de acceso públicos (*hotspots*) este ataque se ha popularizado. El atacante solo tiene que disponer de un punto de acceso en el mismo lugar en el que se encuentre una red inalámbrica pública legítima.

Cuando el punto de acceso del intruso comience a funcionar, emitirá señales indicando su disponibilidad. Muchos sistemas operativos actuales están diseñados para conectarse a la red inalámbrica que más le convenga por defecto y sin avisar al usuario. Ello implica que, si la red del atacante emite con una señal más potente que a la red a la que se conecta la víctima, el sistema operativo puede desconectarse de la red legítima y engancharse a la red del atacante de forma totalmente transparente para el usuario.

Una vez en la red del atacante, entre otras posibilidades, éste tiene control sobre la navegación del usuario. Por ejemplo, puede proporcionarle valores DNS falsos en su configuración TCP, de forma que resuelvan hacia servidores falsos. En esta situación la víctima está expuesta a todo tipo de engaños porque creerá estar visitando una web que en realidad, puede pertenecer al atacante.

Para evitarlo, se deben comprobar siempre que sea posible, los certificados de páginas y de la conexión, y evitar que el sistema operativo se conecte automáticamente a redes desconocidas. Para ello, en la configuración de las redes inalámbricas, se puede determinar si se desea configuración automática o manual.

Ilustración 2: Configuración de las redes inalámbricas en Windows Vista



Fuente: INTECO

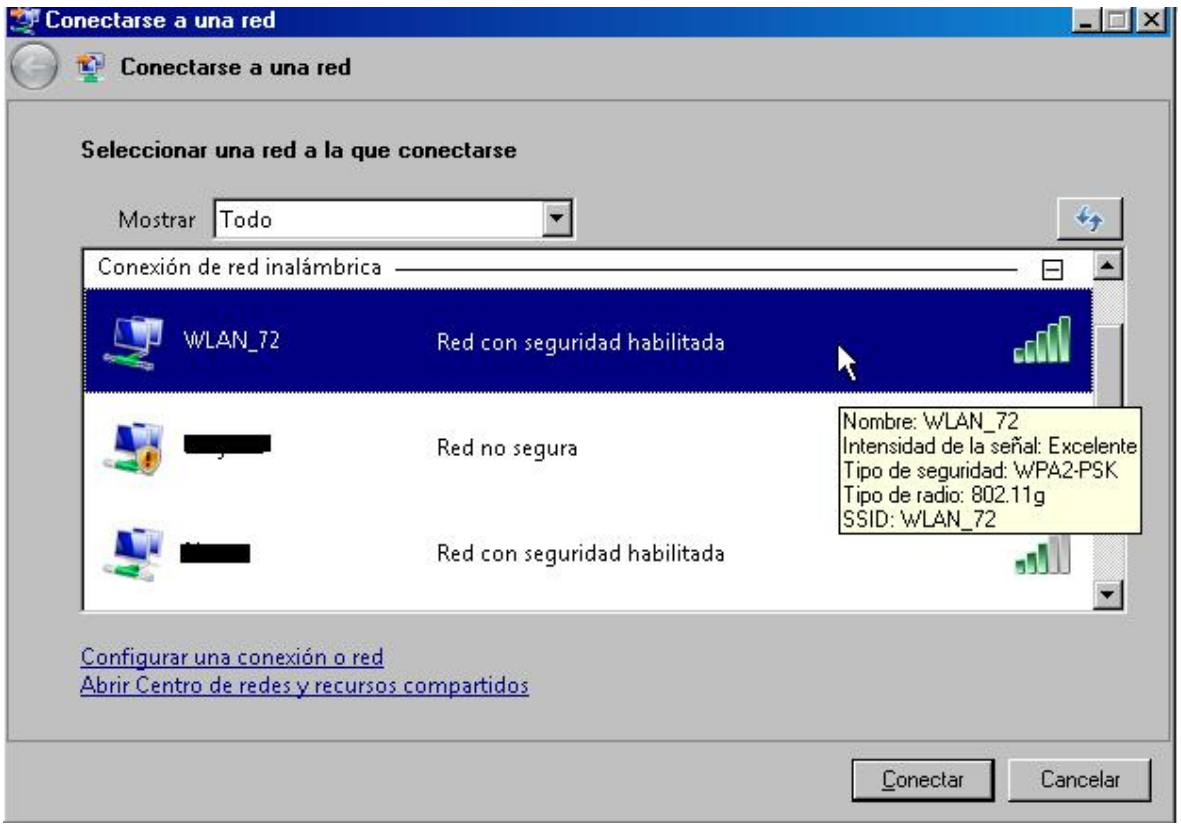
En la administración de redes inalámbrica de Windows, es posible definir los parámetros:

- *Conectarse automáticamente a esta red cuando esté dentro del alcance.*
- *Conectarse a una red preferida, si está dentro del alcance.*
- *Conectarse aunque la red no sea de difusión.*

Es importante indicarle al sistema operativo que no se conecte automáticamente a redes inalámbricas que no sean preferidas (son redes preferidas aquellas a las que el usuario se ha conectado con anterioridad). Para ello, se debe desmarcar, en la configuración de redes inalámbricas, la opción *Conectarse automáticamente a redes no preferidas*.

También es importante entender la terminología de conexión. En Windows Vista y 7, las "Redes con seguridad habilitada" son las que están cifradas con WEP, WPA o WPA2. Las cifradas con WEP, aparecen señaladas con un escudo marcado con una admiración como indicador de que son inseguras. Es importante evitar su uso. Para saber si realmente una red está cifrada con WPA o WPA2, se puede, simplemente, mantener el cursor sobre la red.

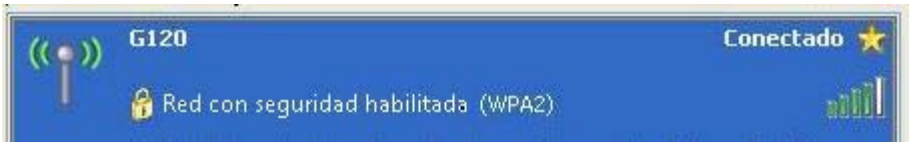
Ilustración 3: Redes inalámbricas disponibles en Windows Vista



Fuente: INTECO

En cambio, en Windows XP las redes que usan WPA o WPA2 aparecen además con un candado y un indicador entre paréntesis de la tecnología. Las redes WEP, sin embargo, no aparecen con escudo alguno.

Ilustración 4: Redes inalámbricas disponibles en Windows XP



Fuente: INTECO

Wardriving

Es el método más conocido para detectar redes inalámbricas inseguras. Los atacantes lo realizan con un dispositivo móvil (como ordenador portátil o PDA) y el software adecuado, disponible de forma gratuita. En el momento en que el intruso detecta la existencia de la red, realiza un análisis para comprobar sus métodos de cifrado y sus mecanismos de seguridad.

Con la popularización de las redes inalámbricas y del uso de WEP como sistema de cifrado, surgió el *wardriving* como forma de explotación de sus debilidades. Incluso, se inventó un lenguaje llamado *warchalking*, un código de símbolos utilizado para marcar sobre el terreno (normalmente con tiza sobre el asfalto) la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por otros que deseen hacer un uso ilegal de ellas.

Ataques específicos contra WEP

El número de ataques posibles contra WEP es muy elevado. Existen suites completas que permiten aprovechar todos los errores de esta tecnología con solo pulsar un botón.

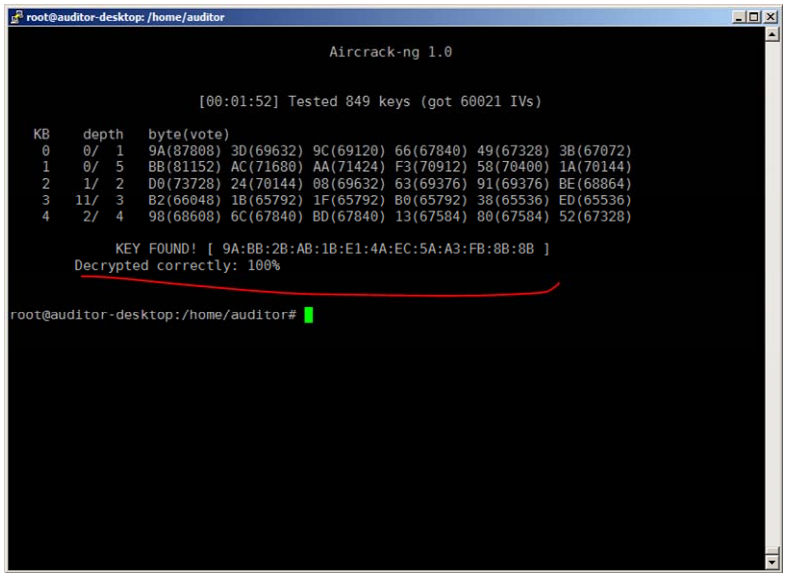
Ilustración 5: Página de *aircrack-ng*, el sistema de crackeo de inalámbricas más popular

Fuente: INTECO

Con una combinación de las técnicas descritas, se pueden realizar ataques que descubren la clave en cuestión de minutos.

Ya a principios de 2005, durante una conferencia en Estados Unidos, tres investigadores del FBI demostraron que podían romper el cifrado WEP con clave de 128 bits de una red inalámbrica en tan sólo tres minutos[1].

Ilustración 6: Resultado del crackeo de una red WEP por *aircrack-ng*



Fuente: INTECO

[1] http://www.hispasec.com/unaaldia/2398

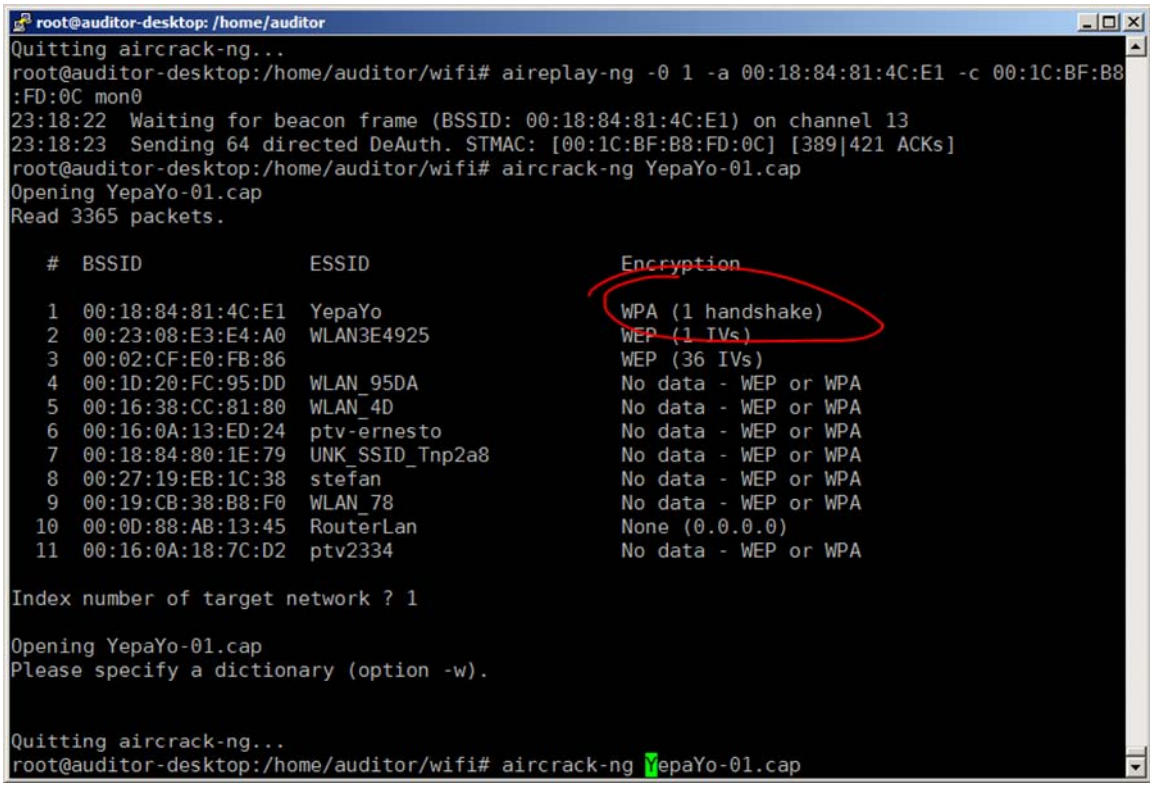
Ataques específicos contra WPA y WPA2

A principios de octubre de 2008 se publicó la noticia de que la compañía rusa ElcomSoft había conseguido reducir sustancialmente el tiempo necesario para recuperar una clave de WPA, ayudándose de tarjetas gráficas NVIDIA[2]. El método conseguía deducir claves de manera extraordinariamente rápida, utilizando fuerza bruta. Ello no implica una debilidad del WPA en sí mismo, por tanto el cifrado se mantenía relativamente a salvo siempre que se usase una contraseña suficientemente larga y entrópica.

Este ataque se realiza sobre una captura de tráfico que el atacante debe conseguir en el momento de la autenticación. Una vez más, *aircrack-ng*, permite realizar este ataque sin esfuerzo.

Este ataque se realiza sobre una captura de tráfico que el atacante debe conseguir en el momento de la autenticación. Una vez más, *aircrack-ng*, permite realizar este ataque sin esfuerzo.

Ilustración 7: Captura del tráfico de autenticación WAP con *aircrack-ng*



Fuente: INTECO

[2] http://www.hispasec.com/unaaldia/3670

Un problema más grave, en esta ocasión inherente al protocolo, se anunció en noviembre de 2008. Los investigadores alemanes Erik Tews y Martin Beck eludieron parcialmente la seguridad de WPA. El método descubierto no permitía recuperar la contraseña. Estaba limitado a descifrar paquetes concretos o inyectar nuevos (y sólo una pequeña cantidad). El ataque sólo funcionaba si se utiliza el protocolo TKIP, no el CCMP (que utiliza cifrado AES). El ataque permitía provocar una denegación de servicio o inyectar paquetes ARP, lo que podría hacer que se redirigiese el tráfico.

Un ataque basado en la misma técnica que volvió obsoleto al WEP permitió que se pudiese descifrar un paquete de tipo ARP en menos de 15 minutos, independientemente de la contraseña usada para proteger el WPA.

En agosto de 2009, dos investigadores japoneses descubrieron una manera de reducir el tiempo de ataque. Toshihiro Ohigashi (Universidad de Hiroshima) y Masakatu Morii (Universidad de Kobe) consiguieron realizar el ataque en un minuto prescindiendo de la limitación del anterior: el soporte de características de QoS[3].

En el verano de 2010 se descubrió el problema en WPA2 conocido como "Hole196"[4]. Su nombre proviene de que la vulnerabilidad se produce por un error en la descripción oficial del protocolo que define WPA2. De sus 1232 páginas, en la 196 se obviaba un detalle que, convertido en problema de seguridad, podría permitir a un atacante interno hacerse con la red.

A grandes rasgos, el fallo se encuentra en el *Group Temporal Key* (GTK), compartido por todos los clientes autorizados en una red protegida con WPA2. Según define el protocolo, solo un punto de acceso podría trasmitir datos cifrados al grupo usando la GTK. Pero en el estándar no se dice que un cliente no pueda falsificar estos paquetes y enviarlos al grupo. Así, un atacante ya autenticado en la red, podría llegar a descifrar información del resto de usuarios.

Aun así, incluso con los ataques conocidos hasta el momento, el uso de WPA2 bien configurado es lo más seguro que se conoce hoy día para proteger redes inalámbricas.

[3] http://www.thestandard.com/news/2009/08/26/new-attack-cracks-common-wi-fi-encryption-minute

[4] http://www.airtightnetworks.com/WPA2-Hole196