Proteger una red Wireless

Autor: Chema Alonso

http://elladodelmal.blogspot.com/

Recopilación: Lic. Cristian Borghello, CISSP

Fecha Publicación: 23 de agosto de 2008

Estos documentos han sido escritos y publicados por Chema Alonso

Indice

Proteger una red Wireless

http://elladodelmal.blogspot.com/2006/10/proteger-una-red-wireless-i-de-iii.html

Atacar redes Wireless se ha convertido desde hace tiempo en un deporte, una diversión o un hobby. En casi todos los medios de comunicación se han escrito artículos sobre como hackear redes Inalámbricas (yo mismo escribí un artículo sobre esto mismo hace casi 2 años) e incluso en los Microsoft Security Days del año 2005 y la gira de Seguridad Technet fuimos haciendo demostraciones de cómo se puede realizar de forma sencilla un ataque a una red Wireless.

Sin embargo, sigue siendo común que los ataques a redes Wireless tengan éxito. ¿Por qué sucede esto? Justificaciones como ¿Quién me va a atacar a mi? O Si yo no tengo nada importante, me da igual que usen mi red suelen ser reflejo de una falta de conocimiento del riesgo o un problema de conocimiento técnico de cómo se puede securizar una red inalámbrica. Vamos a hacer un rápido repaso a las tecnologías de seguridad en las redes Wireless y viendo los riesgos que tienen cada una de ellas para poder elegir una buena opción a la hora de proteger nuestra red.

La tecnología Wireless

Cualquier conexión que se realice sin cables se considera inalámbrica, pero nosotros nos vamos a centrar en las redes WLan, o redes de área local Wireless. Las redes inalámbricas pueden ser de dos tipos, Ad-hoc, que sería una red entre dos equipos iguales (red de pares) o de Infraestructura, que simularía una conexión de red basada en un Hub o concentrador de conexiones. Esto es importante porque mediatiza los tipos de ataques que se pueden realizar.

Los estándares que gobiernan estas tecnologías son los 802.11 y los primeros que llegaron al público fueron los 802.11b y 802.11g, estándares que permitían velocidades de transmisión desde 11 Mb/s hasta 108 Mb/s. Desde el año 2004 se trabaja en el estándar 802.11n que permitirá implementaciones de hasta 500 Mb/s y que se espera que esté publicado a finales de este año o principios del 2007. Sorprendentemente, al igual que sucedió con la espera del 802.11i (que hablaremos de él un poco más adelante) ya se ha adelantado el mercado y están disponibles a la venta dispositivos 802.11n que se han diseñado siguiendo la información en el borrador [1] del estándar que se aprobó. Para completar algunas de las “letras” que podemos encontrarnos en los estándares, existe la versión 802.11e, pensada para transmisión de video y audio en tiempo real mediante la utilización de protocolos de calidad de servicio.

Vale, hasta aquí información sobre “letras” que nos marcan algunas características de las conexiones, pero no de la seguridad. Sigamos adelante.

Definición de una WLan

Lo primero que debemos definir es el nombre de nuestra red WLan, y para ello unas breves definiciones para aclararnos:

- BSS (Basic Service Set). Se refiere a un conjunto de máquinas que pertenecen a una misma red inalámbrica y que comparten un mismo Punto de Acceo a la red Wireless (AP)

- BSSID (Basic Service Set Identifier): Es el identificador que se usa para referirse a un BSS. Tiene la estructura de dirección MAC y generalmente todos los fabricantes utilizan la dirección MAC del AP. Esto es importante, porque los atacantes descubren este valor para poder identificar los clientes de la red. Para ello, los atacantes buscan en las comunicaciones de red que máquinas se están conectando con ese AP.

- ESS (Extended Service Set). Es un conjunto de BSS que forman una red, generalmente será una Wlan completa.

- SSID (Service Set Identifier): Es el nombre de la Wlan, entendible para el usuario, el que nosotros configuramos: mi_wlan, escrufi o wlan1.

- ESSID (Extender Set Service Identifier): Es el identificador del ESS, es transparente al usuario y lleva la información del SSID.

Al final, cuando configuramos una Wlan, lo que debemos hacer es seleccionar un nombre para nuestro SSID y un canal de radio para la frecuencia de comunicación.

Ocultación SSID

El SSID es necesario para establecer una comunicación, es decir, cuando un cliente se quiere conectar con el AP necesita conocer el SSID de la red. El estándar para wlans permite dos formas de trabajar con el SSID:

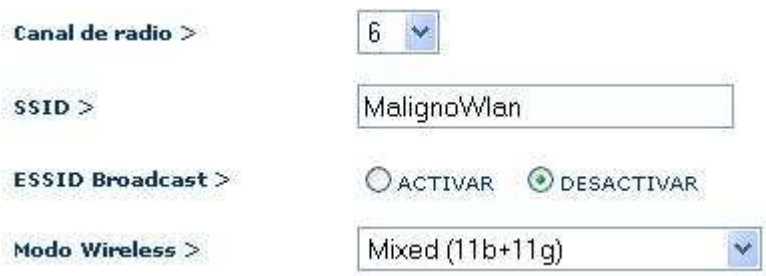
- Descubrimiento Pasivo: El cliente recibe una trama baliza (Beacon frame) con la información del SSID. El AP difunde constantemente unas tramas de información con el ESSID donde va la información del SSID de la red.

- Descubrimiento Activo: El cliente tiene que conocer el SSID porque el AP no ofrece beacom Frames.

Esta no es una medida de seguridad ya que descubrir el SSID de una wlan es trivial para un atacante que solo tiene que esperar a que un equipo cliente envíe información para conectarse y ver el SSID.

Pero incluso el hacker no necesita ser paciente y esperar a que un equipo se conecte y puede realizar lo que se llama el ataque 0, es decir, enviar una trama de gestión al cliente, simulando ser el AP (spoofeando la mac de origen) que le pide que se desconecte. El cliente, muy cumplidor con el estándar, se desconecta e intenta conectarse con el siguiente AP del ESS. Si sólo hay un AP, entonces se conectará con el mismo. Durante este proceso el hacker descubrirá el SSID de la wlan.

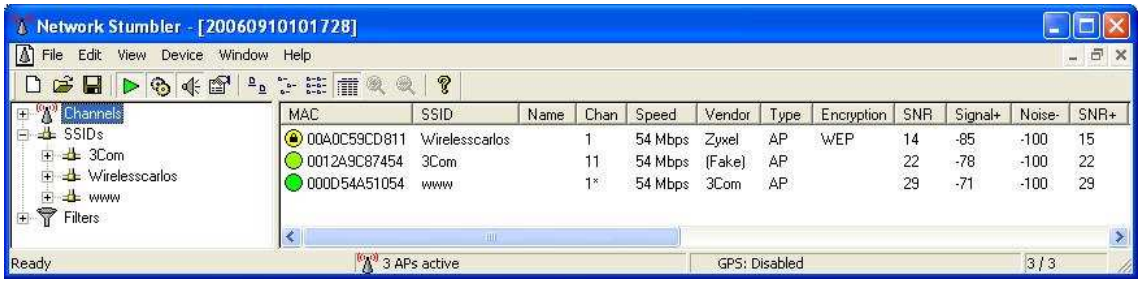
Conclusión: Activar o no el ESSID Broadcast es una opción de comodidad y/o contaminación del espectro de radio. No es una medida de seguridad.



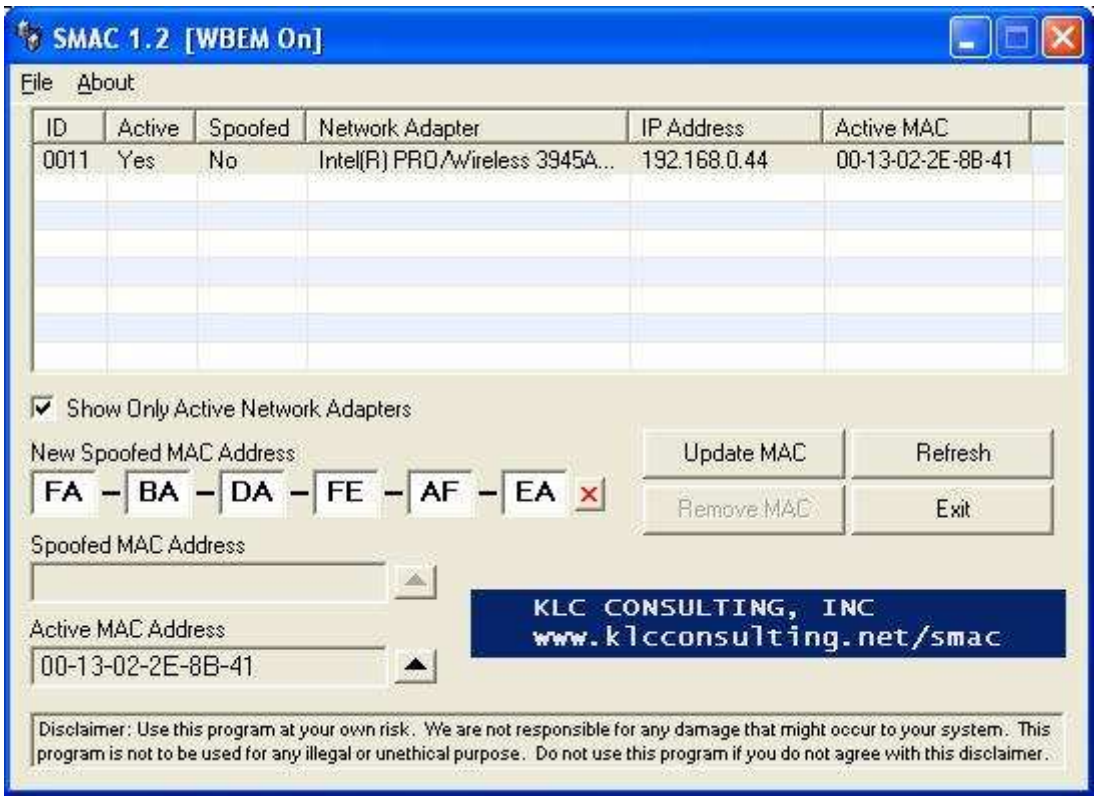
Protección MAC

Para evitar que se conecten clientes no deseados muchos AP ofrecen opciones para crear listas blancas de equipos que se pueden conectar en función de la dirección MAC de los clientes. Para ello en el AP se añaden las direcciones de las máquinas que queremos permitir y listo.

Esto no es una medida de seguridad robusta pues es bastante fácil de saltar para un atacante. Utilizando cualquier herramienta de análisis de redes wlan com Netstumbler nos descubren los SSID, el canal y frecuencia que está siendo utilizado y la MAC del AP.



Una vez que se conocen las MACs de los AP conocer las Macs de los clientes autorizados es tan sencillo como abrir un Sniffer de red como AiroPeek y ver que direcciones se comunican con la MAC del AP. Esas serán las MACs autorizadas. Cuando ya se tiene la lista de las direcciones autorizadas, pues el atacante se configura una MAC válida con alguna de las muchas herramientas que hay para spoofear(suplantar) direcciones y ya se habrá saltado esa protección.



Conclusión: El filtrado de direcciones MAC no es una buena protección de seguridad, es muy sencillo para un atacante saltarse está protección.

Autenticación y Cifrado

Claves WEP 64 y 128 bits

El estándar 802.11 define un sistema para Autenticación y cifrado de las comunicaciones Wlan que se llama WEP (Wireless Equivalent Privacy).

WEP utiliza una palabra clave que va a ser utilizada para autenticarse en redes WEP cerradas y para cifrar los mensajes de la comunicación.

Para generar la clave, en muchos AP se pide una frase y luego a partir de ella se generan 5 claves distintas para garantizar el máximo azar en la elección de la misma, pero en otros simplemente se pide que se introduzca una con las restricciones de longitud que se configure y listo.

Para el cifrado de cada trama se añadirá una secuencia cambiante de bits, que se llama Vector de Inicialización (IV), para que no se utilice siempre la misma clave de cifrado y descifrado. Así, dos mensajes iguales no generarán el mismo resultado cifrado ya que la clave va cambiando.

Como se puede ver en la imagen, en este caso tenemos un AP que permite generar 5 claves a partir de una Frase o directamente configurara una clave. Cuando tenemos 5 claves, hemos de marcar cual es la que vamos a utilizar porque WEP solo utiliza 1 clave para todo. Como se puede ver hemos seleccionado una opción de clave WEP de 64 bits, de los cuales 5 octetos (40 bits) son la clave y los 24 bits restantes serán el IV. Es decir, en una comunicación normal tendríamos 2 a la 24 claves distintas de cifrado.

En el caso de WEP de 128 bits tendremos 13 octetos fijos (104 bytes) y 24 bits cambiantes (IV), es decir, tendremos el mismo número de claves pero de mayor longitud.

Proceso de Cifrado y Descifrado

Para entender el proceso de autenticación en redes Wlan con WEP es necesario explicar previamente el proceso de cifrado y descifrado ya que es utilizado durante el proceso de autenticación de un cliente.

El proceso de cifrado es el siguiente:

Paso 1: Se elige el IV (24 bits). El estándar no exige una formula concreta.

Paso 2: Se unen la clave Wep y el IV para generar una secuencia de 64 o 128 bits. Este valor se llama RC4 Keystream.

Paso 3: Se pasa esa secuencia por un algoritmo RC4 para generar un valor cifrado de esa clave en concreto.

Paso 4: Se genera un valor de integridad del mensaje a transmitir (ICV) para comprobar que el mensaje ha sido descifrado correctamente y se añade al final del mensaje.

Paso 5: Se hace un XOR entre el mensaje y el RC4 Keystream generando el mensaje cifrado.

Paso 6: Se añade al mensaje cifrado el IV utilizado para que el destinatario sea capaz de descifrar el mensaje.

El proceso de descifrado es el inverso:

Paso 1: Se lee el IV del mensaje recibido

Paso 2: Se pega el IV a la clave WEP

Paso 3: Se genera el RC4 Keystream

Paso 4: Se hace XOR entre el mensaje cifrado y el RC4 KeyStream y se obtiene el mensaje y el ICV.

Paso 5: Se comprueba el ICV para el mensaje obtenido.

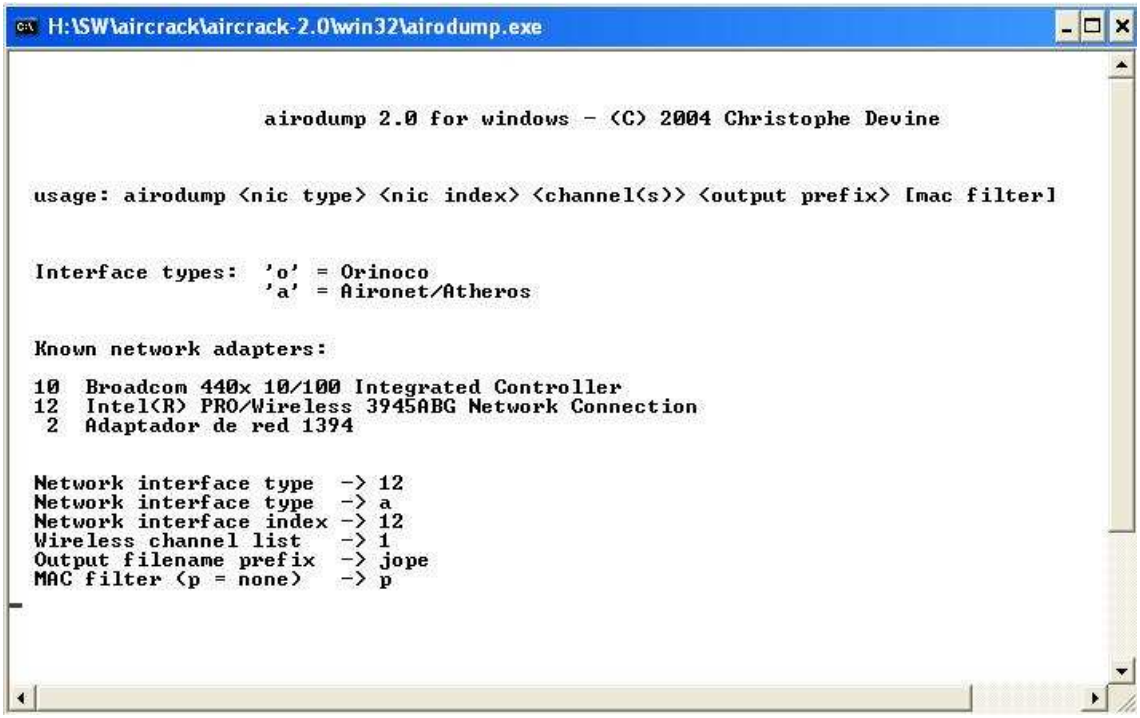
Proceso de Autenticación

A la hora de que un cliente se conecte a una Wlan se debe autenticar. Esta autenticación puede ser abierta, es decir, que no hay ninguna medida de exigencia para que pueda asociarse a la red, o cerrada, por la que se va a producir un proceso de reconocimiento de un cliente válido.

Así, en una autenticación WEP se usa una idea muy sencilla. Si tienes la clave WEP serás capaz de devolverme cifrado lo que te envíe. Así, el cliente pide conectarse y el AP genera una secuencia de 128 octetos que le envía al cliente cifrado. El cilente descifra esa cadena de 128 octetos y se la devuelve en otra trama cifrada con otro IV. Para que la autenticación sea mutua se repite el proceso de forma inversa, es decir, enviando el AP la petición de conexión al cliente y repitiéndose el envío de la cadena de 128 octetos cifrados del cliente al AP.

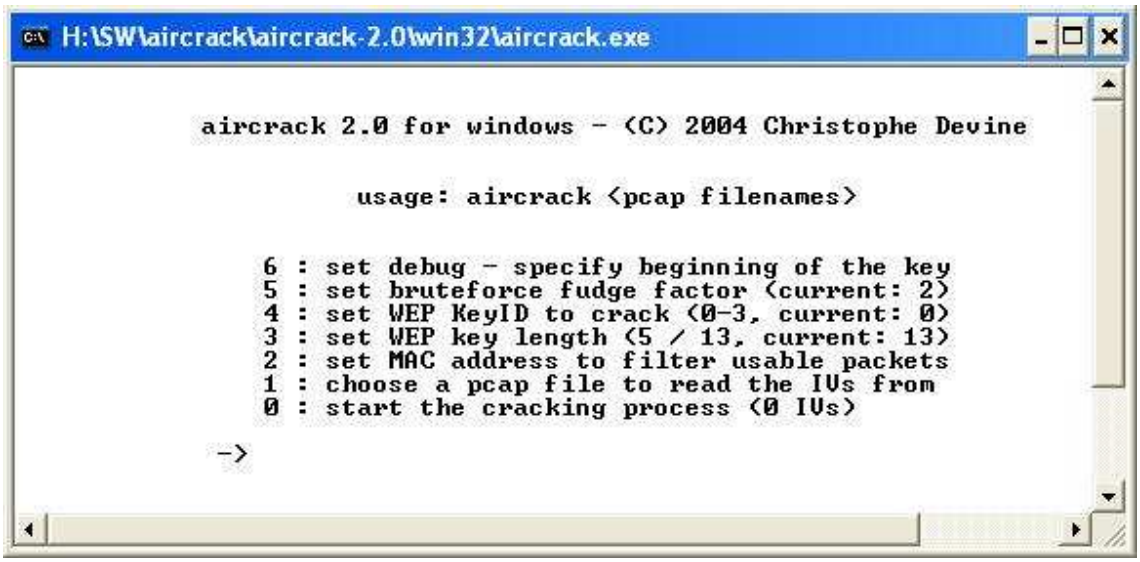
Seguridad WEP

¿Es seguro utilizar WEP entonces? Pues la verdad es que no. Hace ya años que se demostró que se podía romper y hoy en día romper un WEP es bastante trivial y en cuestión de minutos se consigue averiguar la clave WEP. El atacante solo tiene que capturar suficientes tramas cifradas con el mismo IV; la clave WEP va en todos los mensajes, así qué, si se consiguen suficientes mensajes cifrados con el mismo IV se puede hacer una interpolación matemática y en pocos segundos se consigue averiguar la clave WEP. Para conseguir suficientes mensajes cifrados con el mismo IV el atacante puede simplemente esperar o generar muchos mensajes repetidos mediante una herramienta de inyección de tráfico. Hoy en día, para los atacantes es muy sencillo romper el WEP porque existen herramientas gratuitas suficientemente sencillas como para obviar el proceso que realizan para romper el WEP.



Pero incluso aquí en España, donde hay un grupo de investigación sobre el tema de seguridad Wireless (http://hwagm.elhacker.net/) se han desarrollado herramientas con GUI para que sean más sencillitas.

Una vez que han generado un fichero de capturas suficiente se pasa por el crackeador que va a devolver la clave WEP que está siendo utilizada.



WLanDecrypter

Una especificación concreta de las redes WEP se ha producido en España. Una compañía de televisión por Internet instala en sus clientes siempre redes Wireless a las que configura, como SSID un valor del tipo: WLAN_XX.

Estas redes utilizan un sistema de claves WEP sencillo que ha sido descubierto. La clave esta compuesta con la primera letra de la marca del router utilizado en mayúsculas (Comtrend, Zyxel, Xavi) y la MAC de la interfaz WAN del router. Además el nombre de la red es WLAN_XX donde XX son los dos últimos dígitos de la dirección MAC de la interfaz WAN. Como cada router tiene una asociación entre el fabricante de la interfaz wireless y de la interfaz WAN, puesto que se hacen en serie y con las mismas piezas, si sabemos la MAC de la interfaz wireless también sabremos los 3 primeros pares de dígitos hexadecimales de la MAC WAN (que corresponden al fabricante).

En definitiva, con una herramienta sencilla y una captura de 1 mensaje de red en pocos segundos se rompe la clave WEP de este tipo de redes. Hasta que las empresas cambien su política.

Direccionamiento de Red

Para un atacante, encontrar el direccionamiento de red que tiene que utilizar en una wlan en la que se ha colado es también un paso trivial:

- La red cuenta con servidor DHCP: el equipo del atacante será configurado automáticamente y no tendrá que hacer nada. En el caso de que haya suplantado una dirección MAC de un cliente, el atacante no podrá utilizar esta dirección IP porque ya está siendo utilizada por otro (ya que el servidor DHCP asigna direcciones en función de direcciones MAC), pero le servirá para ver el rango de direccionamiento que puede utilizar y la puerta de enlace.

La red con cuenta con DHCP: El cliente se conecta con una dirección IP no valida y realiza capturas de la red con un sniffer (Wireshark, Ethereal, AiroPeek, …). En una captura con tráfico verá rápidamente cuales son las direcciones IP que se están utilizando. Para averiguar la puerta de enlace solo tendrá que buscar una comunicación entre un equipo interno con una IP externa. Ese mensaje, obligatoriamente ha sido enviado a la puerta de enlace, luego la MAC destino de ese mensaje será la MAC de la puerta de enlace. Basta utilizar los comandos ARP para averiguar la IP asociada a esa MAC.

802.11i, WPA y WPA2

Visto lo visto, todo el mundo sabía que había que hacer algo con la seguridad en las redes Wireless. La única solución que se planteaba con este panorama consistía en realizar conexiones VPNs desde el cliente que se quiere conectar a una Wlan hasta un servidor en la red para conseguir cifrar las conexiones, es decir, tratar la Wlan como una red insegura, como Internet, y realizar un cifrado y una autenticación por encima con los mecanismos que nos ofrecen los servidores de VPN.

El IEEE 802.11 anunció una nueva versión segura para Wlan que se llamaría 802.11i y cambiaría los protocolos de seguridad de las Wlans. Como el proceso de aprobación de un estándar era largo y el mercado necesitaba una solución rápida, un grupo de empresas, reunidas bajo la organización Wi-Fi Alliance crearon WPA (Wireless Protected Access) como una implementación práctica de lo que sería el próximo estándar 802.11i.

Riesgos

http://elladodelmal.blogspot.com/2006/11/proteger-una-red-wireless-ii-de-iii.html

A pesar de esto la gente sigue pensando en que no hay demasiados riesgos, así que este mes, vamos a ver que puede realizar un hacker con una red wireless ajena.

Parásito

Al estilo de Venom, el traje alienigena de Spiderman, muchas de las redes Wireless de hoy en día tienen a su/s parásitos viviendo con ellos, es decir, ese o esos vecinos que alegremente se ahorran unos euros a base de utilizar tu conexión. Suele ser el menor de los problemas y a la vez el más incomodo, es como tener una dolencia crónica en nuestra conexión de Internet.

Ejecución de delitos

En este país existen diferentes grupos de investigación de delitos telemáticos dentro de los cuerpos de seguridad. Estos cuerpos se encargan de perseguir las intrusiones de los hackers de gorra negra, o los defacements (grafittis de páginas web) de los crackers o los ataques de denegación de servicio (DOS = Denial Of Service) o "doseos" de los crashers, o….. Su misión es encontrar evidencias de donde puede haber sido la procedencia del ataque y para ello se busca la dirección IP del atacante. Si el hacker ha utilizado técnicas de anonimato basadas en proxys anónimos o redes TOR (The Onion Routing), las direcciones IP serán de exóticos países que impedirán seguir fácilmente la investigación a los equipos de seguridad, pero,... esas técnicas de anónimato suelen ser lentas, la forma más cómoda es bajarse al parque, disfrutar del buen tiempo y usar la dirección IP del router wireless desprotegido de turno. Cuando la Policia y/o la Guardia Civil lleguen a casa del vecino y le precinten el ordenador ya se explicará. ¿Os imagináis que llegan a vuestra casa a precintaros el ordenador por algo que no habéis hecho? Luego a partir de ahí se realiza un análisis forense offline con alguna herramienta tipo Encase y … A lo mejor encuentran, por una tontería cosas que no deberían o… bueno, que me voy, sigamos.

Acceso a Información

Al estar en tu red Wireless, la conexión funciona como un hub, luego todas las comunicaciones que se emitan, si están en el radio de visibilidad de la señal, podrán ser capturadas por el atacante. Así, podrán verse conversaciones de MSN Messenger (que no van cifradas), las transferencias de ficheros que se hagan por estos programitas (fotos, documentos office, música, etc…) e incluso podrán grabar tus conversaciones de voz sobre IP en ficheros mp3 con programas con Ethereal (que graba en .au), orekaudio, el mismo Cain o vomit.

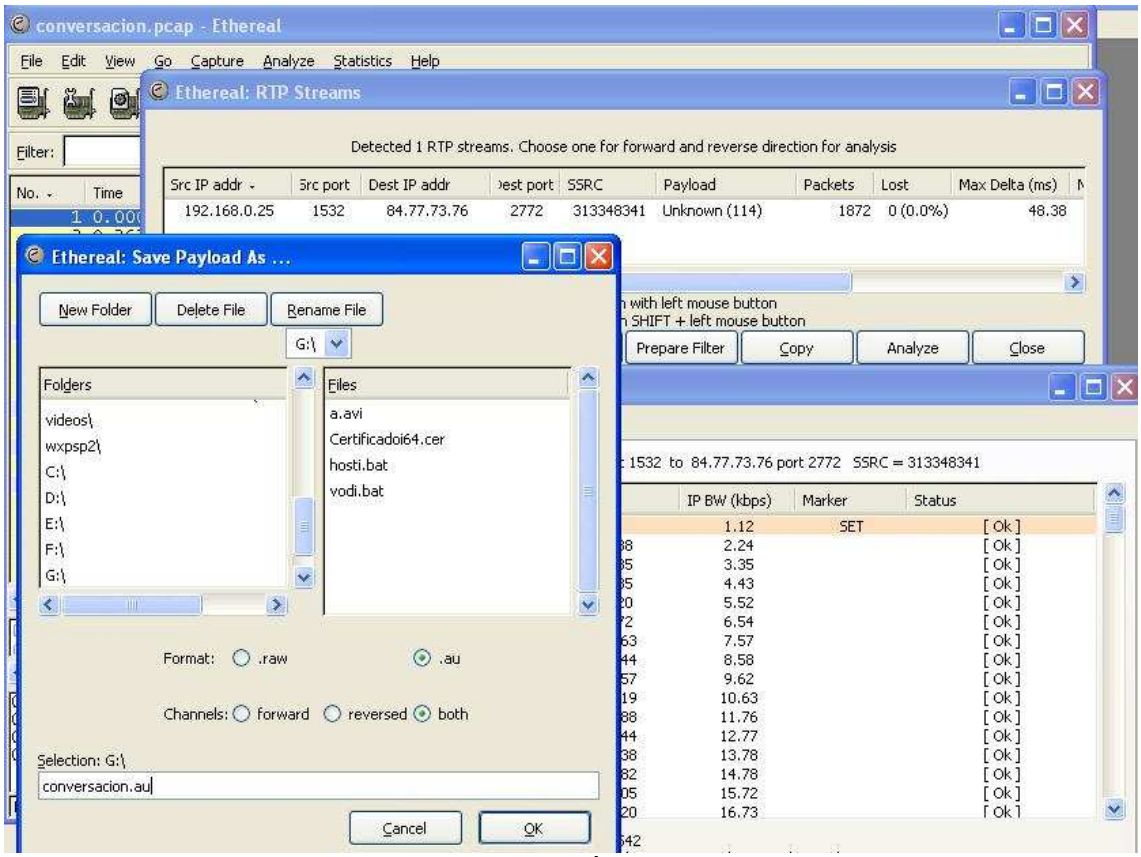
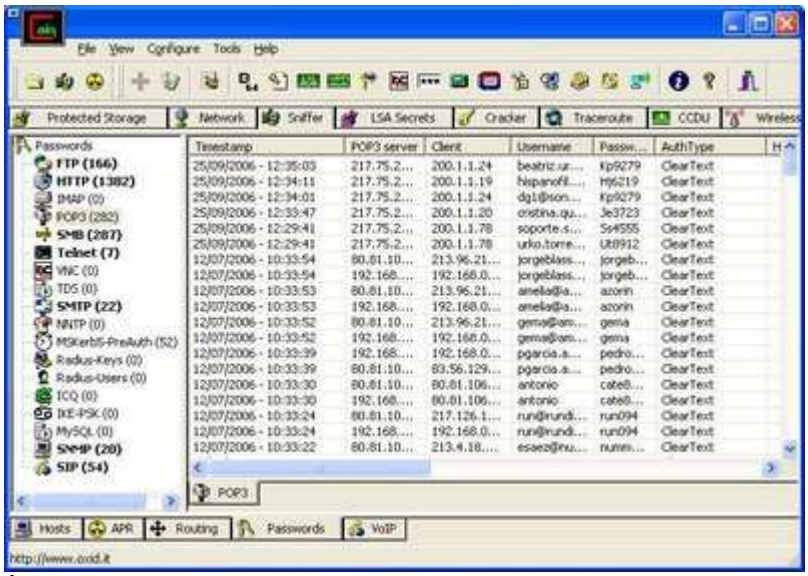


Imagen: Grabando una conversación con Ethereal en fichero .au

Robo de Identidades

Si están en vuestra red wireless ya pueden capturar todo el tráfico que se realice entre vuestro ordenador y el Acces Point, luego, si te conectas a Hotmail, o a un banco o a tu correo electrónico de la empresa o a cualquier sitio con credenciales, el atacante puede robar tus contraseñas con programitas como CAIN, que ya viene con la suite completa para el crackeo de las mismas en caso de que vayan cifradas.



Imágen: Robo de Contraseñas con un Cain “repletito”.

Vale, supongo que esta información ayudará a que queramos securizar las redes wireless y como hemos visto en la primera parte, el mes pasado, la utilización de WEP no es aceptable, así que sigamos viendo las alternativas.

WPA (Wireless Protected Access)

La Wifi Alliance, en el periodo mientras se aprobaba el estándar 802.11i que vendría a sustituir definitivamente a WEP proponía el uso de las siguientes tecnologías de seguridad que ya venían descritas en el borrador de lo que sería el estándar definitivo. José Manuel Alarcón escribió en PCW número 232 de Junio de este año un extenso artículo sobre WPA, así que aquí vamos a ir un poco más directos.

Cifrado WPA

El sistema de cifrado que se utiliza en WPA cambia respecto de WEP (RC4 con claves 64 y 128 bits) a usar TKIP (Temporal Key Integrity Protocol). TKIP sigue usando el protocolo RC4, pero en este caso se minimiza la exposición al ataque utilizando las siguientes modificaciones.

- El Vector de Inicialización (IV) es demasiado corto en WEP, de 24 bits. En TKIP se utilizan IVs de 48 bits. Esto, a priori solo alargaría el proceso, pero seguiría siendo válido el mismo tipo de ataque.

- Integridad datos. En WEP se podía modificar bits en los datos y cambiar el CRC32, es decir, se podían modificar los datos. Para ello se utiliza un nuevo protocolo “Michael” MIC (Messatge Integrity Code) que es cifrado con TKIP

- WEP utiliza la clave principal para cifrar y autenticar. En TKIP se genera una Clave Maestra de 256 bits cuando el cliente se autentica que recibe el nombre de Pairwise Master Key (PMK). Usando PMK más la dirección MAC del AP, la dirección MAC del Cliente y dos números aleatorios, creados uno por el AP y otro por el cliente se generan las claves derivadas. En total TKIP utiliza 6 claves derivadas:
o Data Encryption Key: de 128 bits y utilizada para cifrar los mensajes.
o Date Integrity Key: de 128 bits y utilizada en el protocolo MIC para garantizar la integridad (no modificación) del mensaje.
o EAPOL-Key Encryption Key: Los mensajes EAPOL son los que se usan para autenticar la conexión, y cuando se realizan los procesos de autenticación se utilizan claves especiales.
o EAPOL-Key Integrity Key: De igual forma se utiliza una clave para MIC a parte en los mensajes de autenticación.
o Multicast Encryption Key: 128 bits para cifrar los datos multicast.
o Multicast Integrity Key: 128 bits para garantizar la integridad de los mensajes multicast.

- WEP siempre utiliza las mismas claves. En TKIP se genera un proceso de rekeying periódicamente para generar nuevas claves temporales.- WEP no tiene protección contra Reinyección de paquetes. Es decir, un paquete puede ser capturado y reinyectado en la red, permitiendo aumentar el tráfico. En TKIP esto no se puede hacer porque se usa el IV como contador de protección.

Resumiendo TKIP

El funcionamiento de TKIP se puede resumir de la siguiente forma. Cuando el cliente se autentica se genera una Clave Maestra (PMK) de 256 bits. A partir de ella, utilizando las direcciones MAC del cliente, del AP y dos números aleatorios generados por el cliente y el AP, se determinan 6 claves temporales. Estas claves se usan para cifrar y garantizar los datos transmitidos y además se diferencia entre los mensajes de datos y los de control de autenticación. Cada vez que un cliente se vuelve a autenticar se genera una nueva PMK y periódicamente se cambian las claves derivadas. Además hay control de "replay" de paquetes usando el IV que se ha incrementado de 24 a 48 bits. Hasta aquí sería una fortificación del protocolo WEP, pero además la forma de cifrar y descifrar ha cambiado un poco.

Proceso de Cifrado

Paso 1: Con el IV, la dirección de destino y la Data Encryption Key se genera con un algoritmo de mezcla la Clave de Cifrado de Paquete (Per Packer Encryption Key).

Paso 2: Con la dirección de destino, la dirección de origen, la prioridad del paquete, los datos a enviar y la Data Integrity Key se calcula con el algoritmo Michael el MIC.

Paso 3: Se calcula el ICV (Integrity Check Value a partir del CRC-32).

Paso 4: Con el IV y la Clave de Cifrado de Paquete se genera, con el algoritmo RC4 PRNG el keystream de cifrado que será del mismo tamaño que los datos, el MIC y el ICV.

Paso 5: Se realiza XOR entre el RC4 Keystream y los datos, MIC e ICV para producir el mensaje cifrado.

Paso 6: Se añade el IV al paquete.

La principal diferencia es la utilización de una clave distinta por paquete, que es derivada de una clave temporal (que cambia periódicamente) que a su vez es derivada de la Clave Maestra, que se cambia en cada proceso de autenticación.

Proceso de Descifrado

Paso 1: Se extrae el IV y junto con la Dirección de Destino y la Data Encryption Key se genera la Clave de Cifrado de Paquete.

Paso 2: Con la Clave de Cifrado de Paquete y el IV se genera el RC4 Keystream

Paso 3: Se hace XOR entre el RC4 Keystream y el mensaje cifrado para obtener el mensaje descifrado.

Paso 4: Se calcula el ICV y se compara con el que venía en el paquete para aceptar o descartar el paquete.

Paso 5: Con la Dirección de Destino, la Dirección de Origen, los datos y la Data Integrity Key usamos Michael para calcular el MIC.

Paso 6: Se compara el MIC recibido y el MIC calculado. Si no son iguales se descarta el paquete.

El proceso de descifrado, como se puede ver, es simétrico al de cifrado.

Autenticación WPA

Para autenticar las conexiones Wireless vamos a tener 2 entornos diferenciados, un entorno doméstico y un entorno empresarial.

WPA-PSK

En entornos domésticos solemos tener únicamente un Punto de Acceso (AP) y uno varios clientes. No usamos servidores externos por lo que no vamos a desplegar una infraestructura compleja (¿o sí?). En este entorno utilizaremos una solución basada en clave compartida (Pre-Shared Key) que configuraremos en los clientes y en el Punto de Acceso.

Imagen: WPA en el AP

La elección de la Clave Compartida (PSK) debe ser lo más larga y aleatoria que se pueda (no como la que tenemos en la captura de la pantalla). Esta PSK deberá ser configurada en los clientes y se utilizará para autenticar las conexiones y para generar la Clave Maestra. Un atacante puede, a partir de un paquete de autenticación de un cliente aplicar un algoritmo de fuerza bruta obtener la PSK que le permitirá al usuario autenticarse, pero no le valdrá para obtener la información que está transmitiendo otro cliente ya que los datos de otro cliente irán cifrados por las claves temporales y por lo tanto tendría que averiguar las claves temporales para poder averiguar las claves por paquete y descifrar el tráfico. Estas claves temporales pueden ser averiguadas a posteriori y averiguar el tráfico que ha sido transmitido. Si utilizamos una clave de 63 caracteres aleatorios el tiempo de ruptura por fuerza bruta hace inviable este tipo de ataques. Si por el contrario la contraseña es corta, un atacante que capturase el paquete de autenticación (handsake o saludo) podría lanzar un ataque de diccionario o fuerza fruta con el programa AirCrack.

Imagen: Ataque de diccionario Aircrak a WPA-PSK

Configuración del Cliente WPA-PSK

Para configurar un cliente WPA-PSK en MS Windows XP bastará con configurar las propiedades de una nueva red inalámbrica seleccionando la opción WPA-PSK como sistema de autenticado, TKIP como sistema de cifrado y establecer la Clave Compartida en cada uno de los clientes:

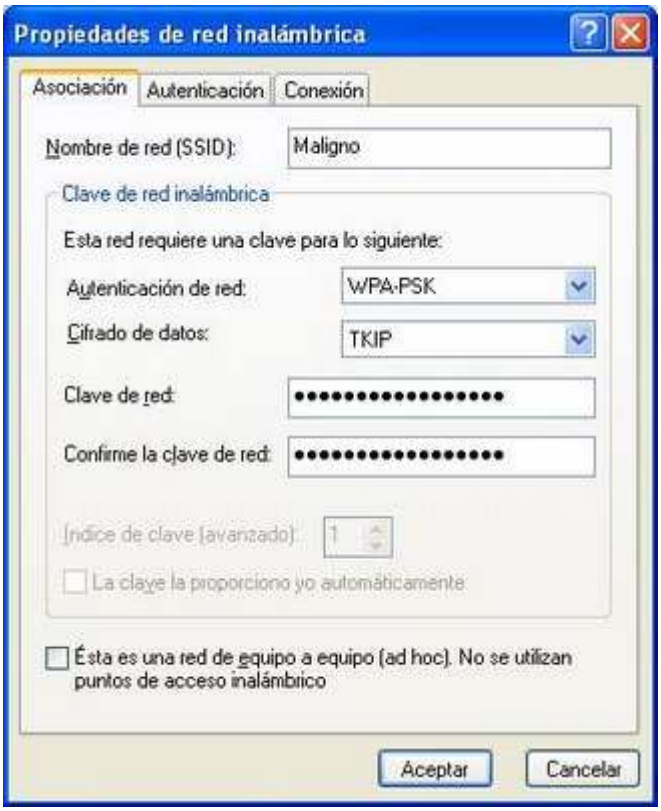


Imagen: Cliente WPA PSK

EAP (Extensible Authentication Protocol)

EAP nació como una evolución de PPP (Point to Point Protocol) que permitiera negociar el sistema de autenticación entre el Cliente o también llamado Suplicante y el Servidor de Autenticación. A diferencia de PPP, en EAP primero se establece la conexión, después se negocia el método de autenticación (EAP Method) entre el Suplicante y el Servidor de Autenticación y por último se concede el acceso o se deniega la conexión. Esto permite que los clientes puedan ser autenticados de diferentes formas por un mismo servidor siempre y cunado ambos estén de acuerdo en el método de autenticación. EAP permite diversos métodos de autenticación pero los más comunes son:

- EAP – MD5 – CHAP: En este método utilizamos un desafío respuesta con la contraseña cifrada en MD5 y mecanismo CHAP. Este mecanismo no se suele utilizar en conexiones inseguras (redes públicas) y se reserva solo a líneas dedicadas y por motivos de compatibilidad con versiones antiguas debido a que CHAP ha sido vulnerado.

- EAP–TLS: Utilizamos como credencial de cliente un certificado de usuario. Así, cualquier usuario que quiera autenticarse no deberá presentar su contraseña sino un certificado digital.

- Protected EAP (PEAP): Con este método, previamente a la negociación EAP entre el cliente o suplicante y el servidor de autenticación se establece un canal seguro TLS, similar al que se utiliza en HTTPs, por lo que es necesario que nuestro Servidor de Autenticación posea un certificado de servidor. Una vez establecido ese canal se procederá a la sesión EAP, que podrá ser:

o PEAP–MSCHAP v2: Al igual que en el método anterior primero se establece un canal TLS entre el Suplicante y el Servidor de Autenticación y después comenzará una sesión desafío respuesta con MS CHAPv2 para autenticar al cliente.

o PEAP–TLS: De nuevo estamos ante un método que utiliza el canal seguro TLS antes de enviar la credencial del suplicante. En este caso la credencial que presentará el cliente será un certificado digital. En este método tendremos que utilizar un certificado de servidor para establecer el canal TLS previo a la sesión EAP y luego un certificado digital para el cliente para poder autenticarlo.

Estos son los métodos que podemos utilizar para autenticar nuestras conexiones, para cada uno de los que elijamos deberemos establecer los mecanismos adecuados, así, si utilizamos EAP–TLS deberemos instalar un certificado digital en cada uno de los Suplicantes para autenticarlos, si usamos PEAP-MSCHAPv2 tendremos que tener un certificado digital en el Servidor de Autenticación y si usamos PEAP-TLS serán necesarios certificados digitales en todos los participantes de la comunicación.

Servidor RADIUS (Remote Authentication Dial-In User Service)

RADIUS es un protocolo de autenticación que se ha convertido en un estándar de la industria para validad usuarios a través de diferentes métodos. Las transacciones en cada una de las comunicaciones entre el cliente y el servidor van cifradas con una clave compartida. Esta clave compartida nunca se envía por la red, así, cada petición de autenticación entre un cliente RADIUS y un Servidor RADIUS debe ir cifrada con esa clave compartida.

Cuando queremos establecer un sistema de autenticación de clientes Wireless a una red el cliente RADIUS será el Punto de Acceso y el Servidor RADIUS contendrá la base de datos de clientes que pueden conectarse. Para ello, en el Punto de Acceso deberemos configurar:

- La dirección IP del servidor RADIUS
- El puerto del Servidor RADIUS, generalmente el 1812.
- La Clave compartida.

Imagen: Configuración Servidor RADIUS en el AP

El Servidor RADIUS tendrá configurada la clave compartida para cada uno de los clientes que pueden realizar una petición RADIUS. En el mes que viene acabaremos de montar al infraestructura y veremos como se configura el Servidor Microsoft Internet Authentication Server (MS IAS), que es el servidor RADIUS de Microsoft.

802.1x

Para poder utilizar el sistema EAP en conexiones Wireless es necesario utilizar un protocolo que permita encapsular el tráfico desde la conexión inalámbrica al Servidor de Autenticación. En un entorno común tendremos un Servidor de Autenticación, que tendrá configurada la política de qué Suplicantes pueden o no conectarse a la organización, y que se encontrará dentro de una zona protegida de nuestra red. El Punto de Acceso Wireless tendrá conexión directa al Servidor de Autenticación y es el que demandará un proceso de Autenticación para un determinado Suplicante. 802.1x nace como forma de poder permitir a cualquier elemento de la red (switches, APs, ….) pedir un proceso de autenticación para una conexión que se acaba de producir. 802.1x utiliza EAPOL (EAP Over Lan) porque lo que va a realizar es una encapsulación del protocolo EAP sobre la red privada para llegar al Servidor de Autenticación. Así, como se ve en el gráfico, el proceso sería el siguiente:

Paso 1: Un cliente se asocia al AP utilizando el protocolo 802.11

Paso 2: El Suplicante inicia el proceso de autenticación 802.1x porque el AP no le concede acceso a la red y se elige el EAP-Method.

Paso 3: El Autenticador requiere la Identidad al Suplicante

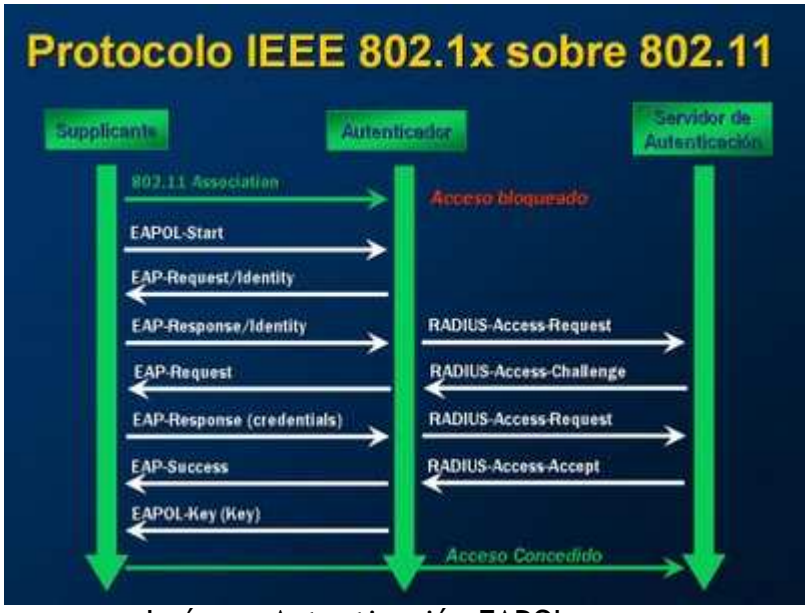
Paso 4: El Suplicante le entrega la Identidad al Autenticador que retransmitirá al Servidor de Autenticación. Como se puede ver, el Servidor de Autenticación es un servidor RADIUS que pedirá las credenciales para esa identidad al Autentcador.

Paso 5: El Autenticador pide las Credenciales al Suplicante.

Pado 6: Suplicante entrega las Credenciales al Autenticador que se retransmiten al Servidor de Autenticación (Servidor RADIUS)

Paso 7: Servidor RADIUS valida las credenciales y Acepta la conexión.

Paso 6: El Autenticador entrega tras aceptar la conexión la EAPOL-Key que no es más que una secuencia de bits que utilizaremos como Clave Maestra en el proceso de cifrado del algoritmo TKIP. Así, cada vez que tenemos un proceso de autenticación o re-autenticación se genera una nueva Clave Maestra.



Imágen: Autenticación EAPOL

Resumen

Hasta el momento hemos visto los riesgos de seguridad que tiene una infraestructura basada en WEP, las características de WPA (Cifrado TKIP, Integridad Michael y autenticado mediante WPA PSK o mediante EAP, RADIUS y 802.1x). El mes que viene terminaremos de montar la infraestructura con el servidor IAS y veremos las características de WPA2 con AES.

IAS (Internet Authentication Service)

http://elladodelmal.blogspot.com/2007/01/proteger-una-red-wireless-iii-de-iii.html

Vamos a terminar de montar la infraestructura WPA, para lo cual vamos a empezar por poner en marcha nuestro servidor RADIUS. Para una organización contar con un servidor RADIUS no es solo una solución segura para conexiones Wireless, también es un elemento importante en la autenticación de conexiones VPN, tanto entre sitios remotos como para clientes o para las soluciones que se nos vienen encima NAP (Network Access Protection) y que en breve estarán implantadas en todos las empresas.

Si la implantación del servidor RADIUS es algo para pocos usuarios o no se desea implantar un servidor dedicado, se puede adquirir fácilmente Routers y/o Access Points Wireless que incluyen dentro de su firmware, pequeños servidores RADIUS con sistema de autenticación EAP-MD5 en la mayoría de los casos. Lógicamente esta es una solución poco escalable ya que, en primer lugar, nos obliga a replicar la base de datos de usuarios dentro del firmware y además, en el caso que contemos con 2 o más Access Point vamos a tener que duplicar estos usuarios en todos los AP o bien pensar en enlazarlos.

Nosotros vamos a implantar como servidor RADIUS la solución de Microsoft, Internet Authentication Service (IAS). Este es que en Windows 2000 Server se proveía como una descarga aparte pero es un servicio que viene "de serie" en Windows Server 2003 y se instala, como cualquier otro, con la opción del panel de control de Agregar o Quitar Programas. Este es un componente de red por lo que habría que seleccionar IAS dentro de estos.

Imagen 1: Instalación componente IAS

Una vez instalado hay que registrar el servidor RADIUS en el Directorio Activo de nuestra organización, y para ello tres opciones, la fácil: desde la consola de administración MMC de IAS, seleccionamos nuestro servidor IAS y elegimos la opción "Regristrar en Directorio Activo" (figura 2); la artesana: Al final, al hacerlo mediante la consola solo se está añadiendo la cuenta de máquina a ciertos grupos privilegiados, por lo que podemos hacerlo manualmente y añadir la cuenta de

máquina de nuestro servidor IAS a los grupos de seguridad IAS y RAS en el Directorio Activo; y por comandos: también se puede realizar el mismo proceso utilizando el comando netsh desde el interfaz de comandos.

Imagen 2: Registrar IAS en Directorio Activo

Una vez registrado ya podemos proceder a configurar nuestro servidor IAS. Tres sencillos pasos a seguir. Primero configurar el registro de conexiones, tanto las correctas como las fallidas para tener una idea de lo que esta sucediendo con nuestra red. Esta es una sencilla operación para detectar los intentos de intrusión o las conexiones "no habituales" de los clientes.

En segundo lugar configurar una Política de Acceso Remoto, es decir, quienes van a poder conectarse remotamente, o lo que es lo mismo en nuestro entorno, quienes van a poder realizar una conexión Wireless. Para terminar la configuración del servidor deberemos establecer cuales van a ser las opciones de conexión, es decir, que mecanismos exigimos para autenticar a los usuarios.

Política de Acceso de Remoto

Con IAS vamos a poder crear políticas de acceso remoto para todo tipo de conexiones, para clientes VPN, para clientes Wireless e incluso para clientes de red, que es en lo que se basa NAP. En este caso vamos a crear una Política de Acceso Remoto para nuestros clientes Wireless y vamos a crearla siguiendo el asistente. Seleccionamos la opción de Política de Acceso Remoto y empezamos:

Imagen 3: Creación de una Política de Acceso Remoto

Una vez introducido el nombre de la política llegamos al cuadro de dialogo donde se nos solicita el tipo de Política de Acceso Remoto que estamos creando, como se puede ver en la imagen tenemos políticas para conexiones VPN, para llamadas de marcado Dial-Up de líneas de telefonía punto a punto, para conexiones Wireless e incluso para conexiones ethernet, que se utilizarán en NAP. Seleccionamos la opción de Wireless, lógicamente, y continuamos hacia delante.

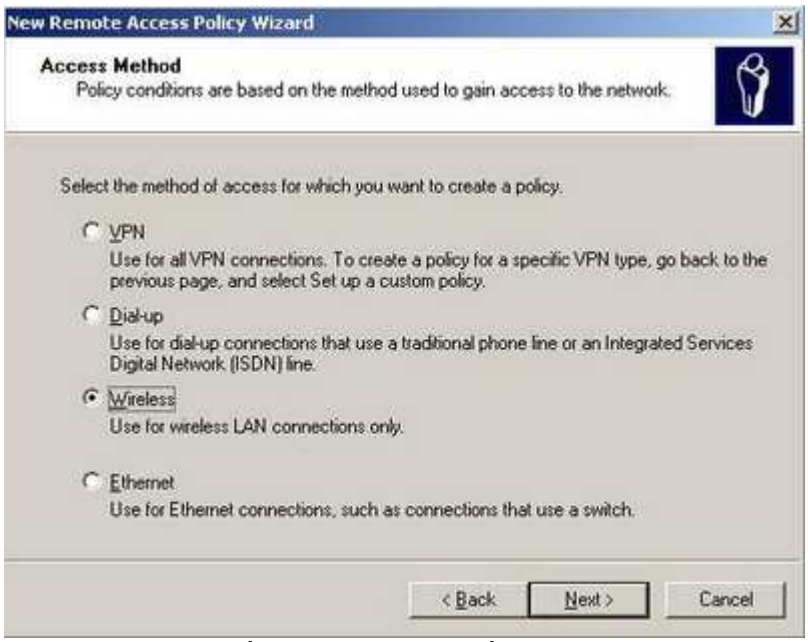


Imagen 4: Selección de tipo de Política de Acceso Remoto

Como nosotros deseamos integrar la seguridad de las conexiones dentro de la infraestructura de nuestra empresa, vamos a crearnos dentro de nuestro Directorio Activo un grupo de usuarios, en este caso llamado “Malos”, (perdón por el chiste), que serán los usuarios que vamos a autorizar con esta Política de Acceso Remoto. Es necesario, que los usuarios tengan el permiso de marcado, igual que para las conexiones de VPN o Dial-Up, ya que es el permiso que se utiliza para las

conexiones remotas. Como esto es un poco engorroso, el seleccionar todos los usuarios y darles ese permiso, se puede utilizar una opción, una vez creada la política con el asistente, en las propiedades que permite ignorar ese permiso y directamente conceder desde IAS el permiso de marcado si cumple la Política de Acceso Remoto.

Imagen 5: Selección de clientes autorizados por esta política

La autorización puede realizarse tanto a nivel de usuarios como a nivel de máquinas por lo que podríamos realizar una autenticación doble, es decir, usuarios autorizados y máquinas autorizadas.

Una vez elegido el grupo de usuarios deberemos elegir el sistema de autenticación. Las opciones a elegir son dos.

Opción 1: PEAP (Protected EAP), que como vimos el mes pasado utiliza un canal TLS generado con el Certificado del servidor, en este caso el del servidor IAS; después elegimos un método de autenticación del cliente que será, o bien contraseña, enviada mediante el protocolo MS-Chap v2, o bien se utilizará directamente un certificado digital del mismo que tendemos en la máquina cliente o una smartcard.

Opción 2: No tenemos canal TLS antes de la autenticación EAP, por lo que utilizamos una autenticación basada en tarjeta inteligente o certificado digital instalado en la máquina cliente.

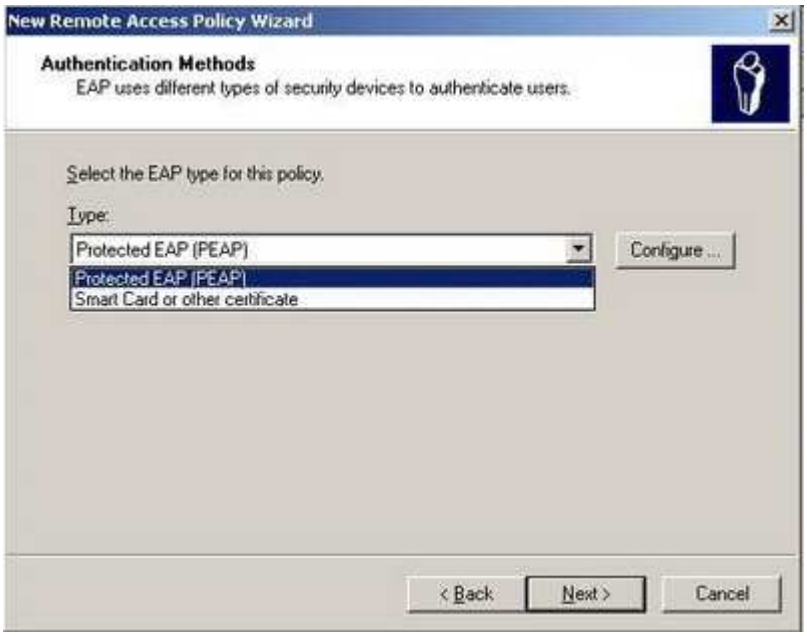


Imagen 6: Selección de método de autenticación de clientes

Con estas opciones hemos terminado de crear la Política de Acceso Remoto para nuestro ejemplo. Hay que notar que se pueden crear tantas políticas de acceso remoto como deseemos. Estas políticas se van a evaluar igual que los firewalls de menor número de orden a mayor y se aplicará la primera que concuerde. Así, podremos tener conexiones autenticadas desde máquinas, o conexiones válidas desde cualquier máquina para algunos usuarios, o conexiones autenticadas con contraseñas porque son dispositivos que no soportan smartcard, etc … a necesidad de la infraestructura.

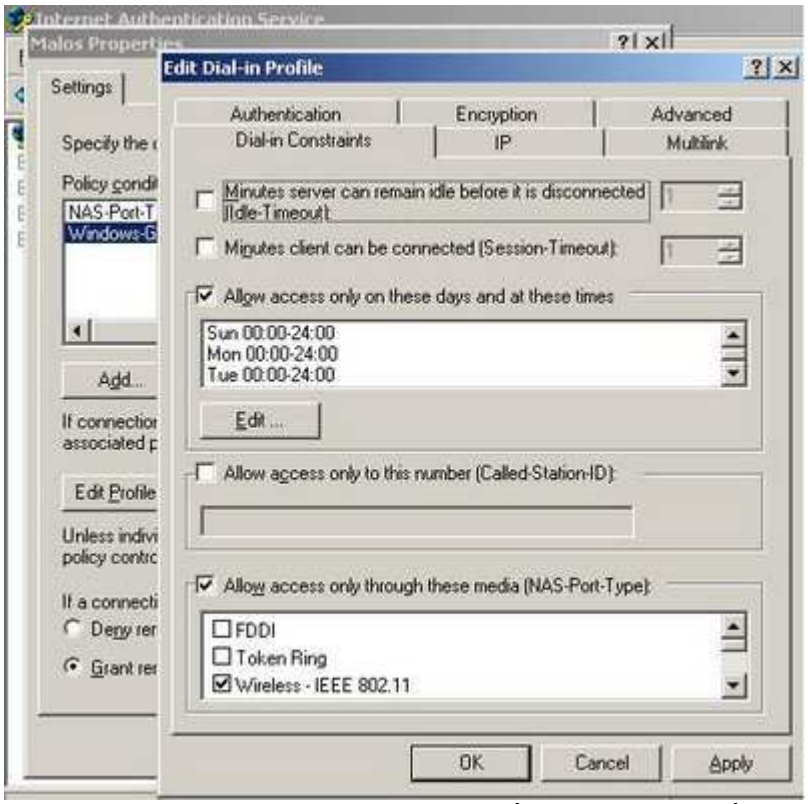


Imagen 7: Propiedades de la Política de Conexión

Una vez creada la política podemos, entrando en sus propiedades, definir algunos valores específicos de la misma, como si hay rangos horarios para la conexión, límites de tiempo, la asignación de direcciones IP, etc… para afinar más las opciones de la política.

Política de Petición de Conexión

Vale, ya hemos creado la política para nuestros clientes Wireless, los que serán o no autenticados con nuestro servidor RADIUS, ahora tenemos que configurar la estructura de autenticación de las peticiones dentro de nuestros servidores RADIUS. Para ello creamos una Política de Petición de Conexión, es decir, cual es el orden de validación de las conexiones en el caso de que tengamos una infraestructura compleja.

La política por defecto que viene creada determina que se autentique en el servidor RADIUS a conexiones que vienen directamente o mediante una conexión VPN utilizando la base de datos del Directorio Activo. Si la autenticación la diera otro servidor RADIUS o si las peticiones vinieran a través de un ISP o se desea comprobar cualquier otro parámetro de la conexión, como por ejemplo, los números de teléfono en una conexión Dial-up o el fabricante de las tarjetas Wireless podemos crear nuevas políticas de conexión. Para nuestro ejemplo, con la política por defecto es perfecto.

Alta de Clientes RADIUS

Ya tenemos definida la Política de Acceso Remoto y la Política de Petición de Conexión, hemos configurado el Registro de Accesos y tenemos el servidor IAS registrado en el Directorio Activo, ¿Qué nos queda? Pues únicamente dar de alta a los puntos de Aceso y/o Routers Wireless que pueden realizar peticiones a nuestro servidor para autenticar clientes. Para ello en la parte de Clientes RADIUS creamos uno nuevo.

Imagen 8: Alta de Clientes RADIUS

Lo primero que se nos solicita es el nombre que le vamos a dar al punto de acceso y cual es la dirección IP o nombre DNS desde la que es accesible para nuestro servidor IAS. En segundo lugar debemos elegir el tipo de cliente RADIUS que es pues a pesar de que existe un estándar, muchos fabricantes han realizado pequeñas variaciones sobre el mismo en la forma de la comunicación.

Imagen 9: Elección de tipo de cliente RADIUS

Por último, lo más importante, el secreto compartido entre nuestro Servidor RADIUS y el cliente. Es la forma de autenticación mutua que se utiliza. Podríamos pensar que es una forma insegura, pues la clave compartida no es la mejor de las formas de autenticar las conexiones, pero se supone, que la conexión física entre el Cliente y el Servidor RADIUS es por una línea privada y securizada.

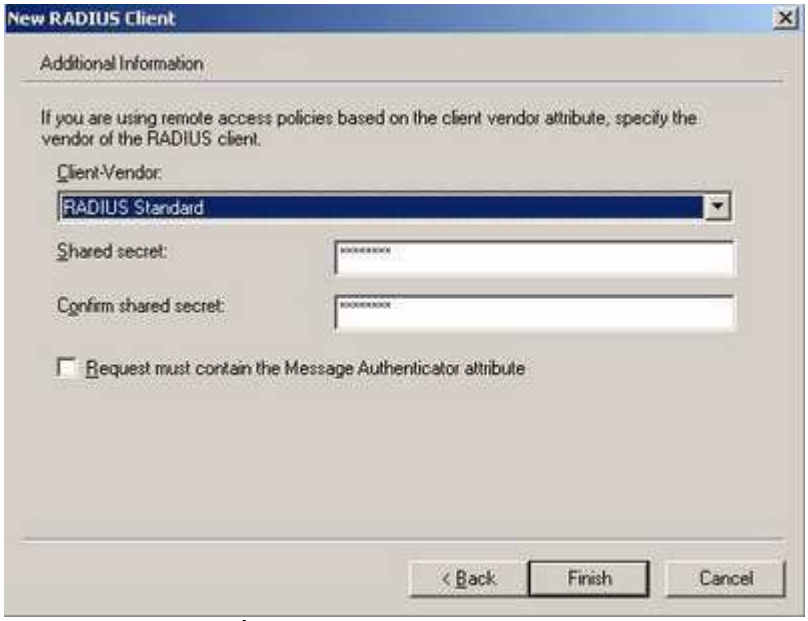


Imagen 10: Configuración de Secreto Compartido para Cliente RADIUS

Al acabar este asistente ya tendremos dado de alta como Cliente RADIUS a nuestro AP, pero este la comunicación no estará funcionando hasta que de forma

simétrica demos de alta al servidor RADIUS en nuestro Punto de Acceso o Router Wireless.

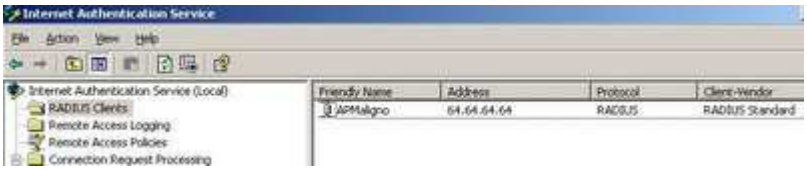


Imagen 11: Lista de Clientes RADIUS en IAS

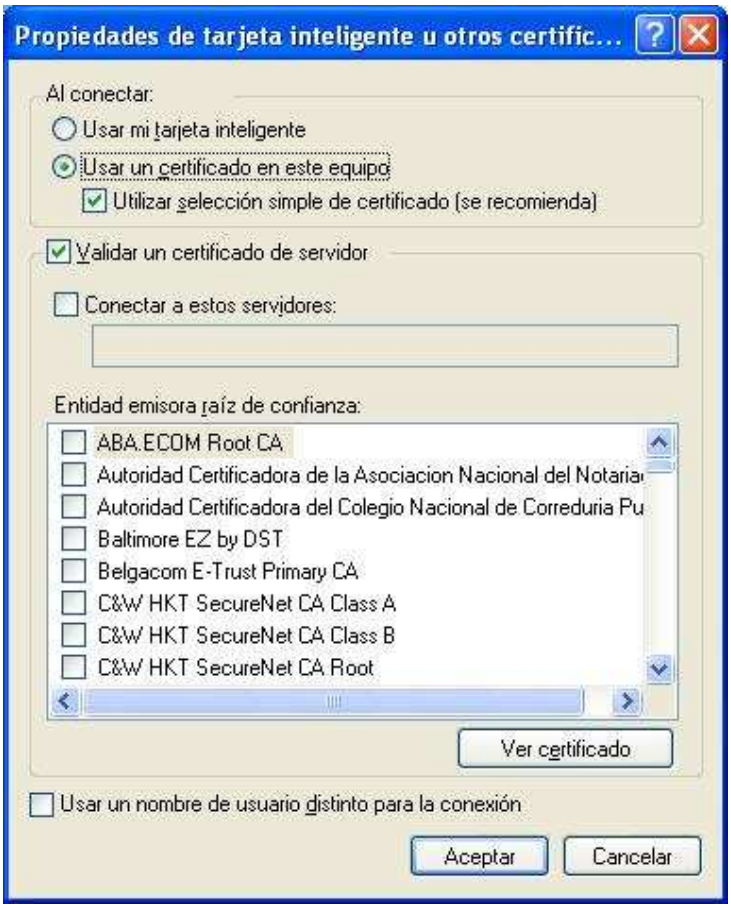
Para dar de alta al servidor RADIUS debemos entrar en la herramienta de administración de nuestro Punto de Acceso Wireless y configurar la dirección IP del servidor RADIUS, el puerto, que por defecto es el 1812 y el secreto compartido. Y ya estaría.

Imagen 12: Configuración del Servidor RADIUS en el AP

Configuración del cliente

Para terminar la conexión en esta infraestructura debemos crear la conexión desde el cliente, para ello entramos en las opciones de la tarjeta de red y damos de alta una nueva red Wireless. Damos de alta el SSID de la misma, seleccionamos la opción de autenticación WPA y de cifrado TKIP. Pasamos en segundo lugar a la parte de Autenticación donde podremos seleccionar “PEAP” o “Certificado Digital o Smartcard”.

Hay que darse cuenta, que en el caso de usar PEAP podremos autenticarnos usando contraseña con MS Chap v2 o con certificado digital o smartcard, mientras que si utilizamos certificado digital o smartcard no podremos utilizar la contraseña. En ambos casos deberemos elegir la entidad certificadora que estamos utilizando para validar todos los certificados digitales, los de servidor y los de cliente, así se puede ver en las propiedades de ambas configuraciones.



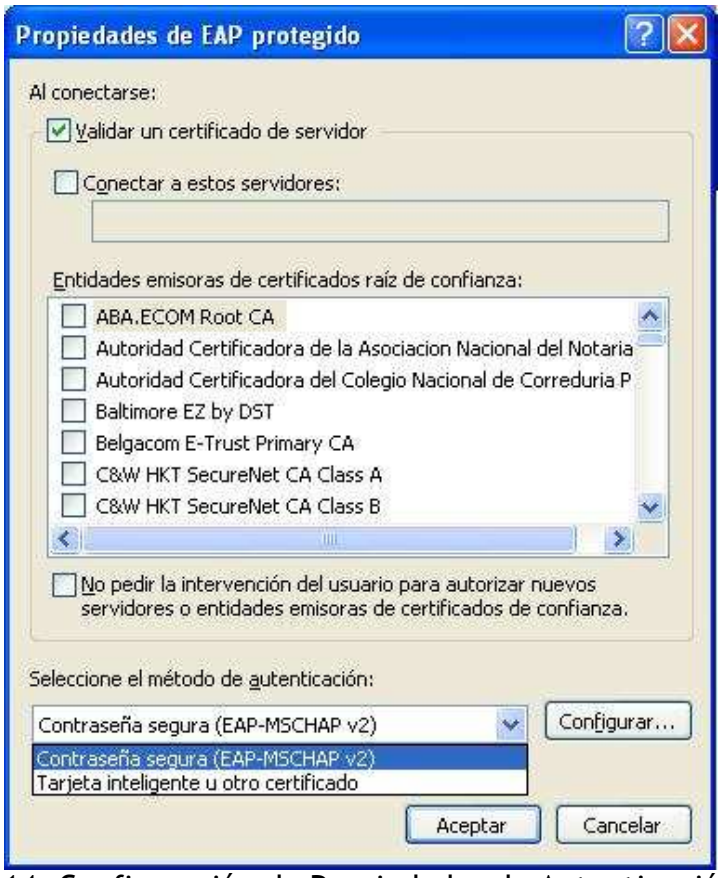


Imagen 14: Configuración de Propiedades de Autenticación

A la izquierda se ve que hemos utilizado Certificado Digital o Smartcard y como debemos seleccionar cual va a ser nuestro certificado y quien es la entidad certificadora que valida los mismos. A la derecha se ve como usamos una entidad para validar el certificado del servidor para crear el tunel TLS y como después, podemos elegir la forma de autenticarnos, con EAP-MSChap v2 o con EAP-TLS.

802.11i y WPA2 (Wi-Fi Protected Access 2)

WPA había nacido sin un estándar que lo apoyara en sus orígenes, pero sí teniendo muy en cuenta lo que iba a ser el estándar 802.11i que vendría a mejorar las soluciones basadas en WEP. Para ello se utilizaron los borradores y la información que se iba obteniendo para ir evolucionando WPA. Cuando ya se tuvo una idea clara de lo que iba a ser 802.11i apareció WPA2. ¿Qué diferencias hay entre WPA y WPA2? La respuesta que se debe decir es que poca y mucha. Mucha en tanto en cuanto está basado en el estándar 802.11i y eso si es un cambio y poca si tenemos en cuenta que WPA estaba ya enfocado hacia ese destino. La principal novedad es el sistema de cifrado que incluye AES.

AES (Advanced Encryption Standard)

AES nació como iniciativa del gobierno americano para sustituir a DES como sistema de cifrado. AES tuvo nombre antes que algoritmo y se estuvo buscando a través de un "mega concurso" mundial cual debía ser el algoritmo a utilizar. Al final se seleccionó Rijndael que tiene ese nombre tan curioso debido a la mezcla de los nombres de los dos creadores. Desde el punto de vista técnico, AES es la opción

que debemos utilizar de cifrado con WPA2, pero la utilización de AES implica el uso de varios algoritmos de cifrado por debajo. Realmente, el algoritmo del estándar 802.11i se llama RSN (Robust Security Network) y es un sistema que negocia el algoritmo de cifrado y autenticación entre las opciones soportadas y configuradas en cliente y servidor. El uso de RSN permite que se pueda negociar con compatibilidad hacia atrás en el caso de ser necesario hacer convivir dispositivos que no soportan AES y usan TKIP o WEP como móviles, PDAs, o sistemas operativos antiguos. RSN soporta WEP, WEP-104, TKIP, WRAP y CCMP que son las implementaciones AES para cifrado de bloque y cifrado de flujo. ¿A que es todo muy sencillito?

La infraestructura empresaria

Para montar una solución de estas características no nos podemos quedar en el montaje manual que hemos utilizado en estos ejemplos sino que deberemos apoyarnos en las utilidades que nos ofrece el Directorio Activo. En primer lugar, para la realización de esta infraestructura hemos supuesto que teníamos realizado un despliegue de certificados de usuario y máquinas dentro de nuestra organización. Es decir, que la infraestructura PKI está subyacente. En segundo lugar hemos realizado las configuraciones de las conexiones de los clientes de forma individual, pero esto se puede automatizar con las políticas.

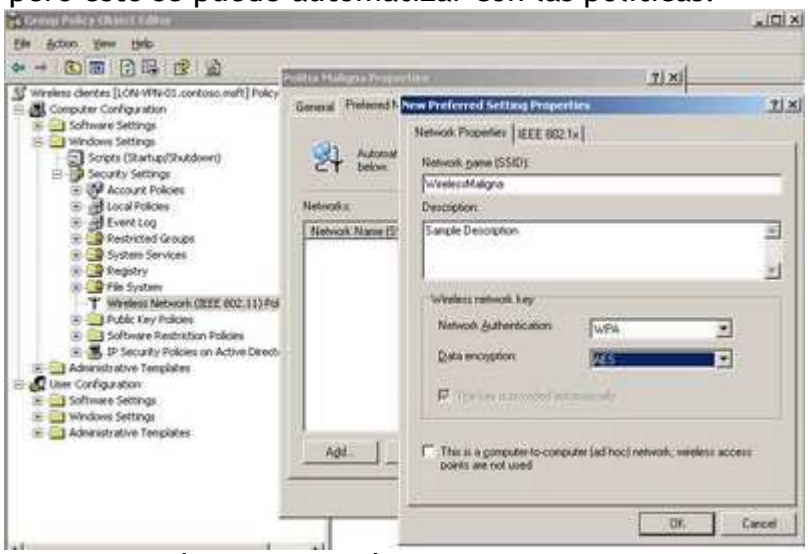


Imagen 15: Creación de una Política Wireless en el Directorio Activo

Para ello creamos una nueva política en la unidad organizativa de las máquinas que queramos configurar para uso de conexiones Wireless y dentro de las opciones de configuración a nivel de máquina creamos una nueva Política de Conexión Wireless. Una vez creada entramos en las propiedades para establecer cuales son las opciones de la conexión Wireless que deseamos crear dentro de los clientes. Allí tendremos que configurar las mismas opciones que hemos visto en la creación de una conexión desde el cliente: SSID, Autenticación, Cifrado, y después las opciones de autenticación.

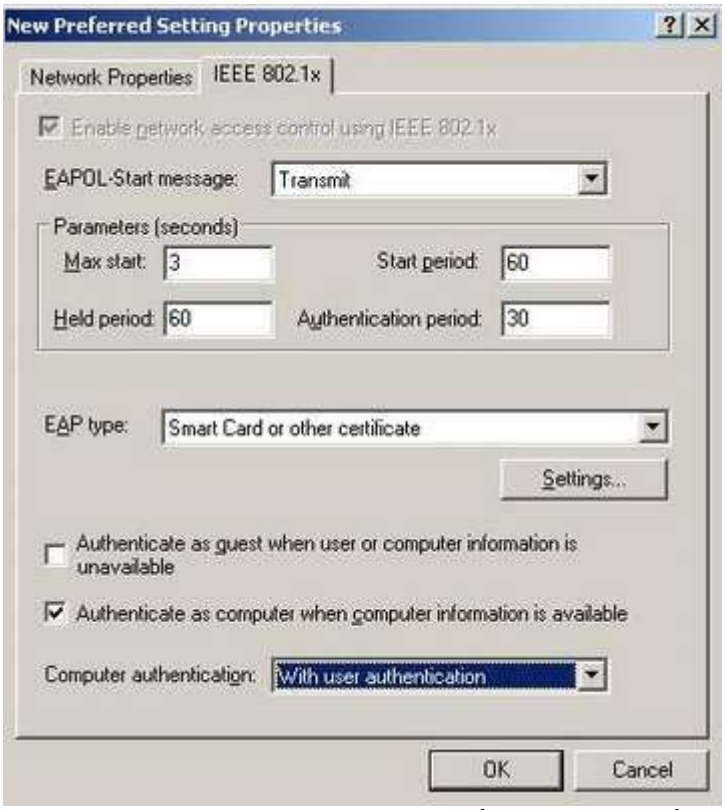


Imagen 16: Opciones de Autenticación para la Política Wireless

Otras Opciones de Securizar una red Wireless

Sí, existen otras opciones para securizar las redes Wireless y las empresas han estado utilizando básicamente dos aproximaciones basadas en lo mismo: Autenticar las conexiones.

Para autenticar las conexiones podemos utilizar un punto de entrada distinto al dispositivo wireless, es decir, en lugar de autenticar en el Access Point, se puede dejar que se conecte el que desee pero después del AP nos encontraremos con la red de la empresa que no permitirá conexiones que no vengan desde un cliente autenticado. ¿Y como autenticamos los clientes válidos?

Opción 1: Con conexiones VPN. Los clientes se conectan al AP y a partir de esa conexión se autentican en el servidor VPN. Una vez que el servidor VPN haya establecido que es un cliente válido ya podrá establecerse en la red.

Opción 2: Mediante certificados digitales e IPSec. Si la red de la organización está desplegada con comunicaciones IPSec, sólo podrá conectarse comunicarse por la red aquel cliente que tenga un certificado digital. Esta opción es menos recomendable debido a que las comunicaciones no cifradas si que pueden ser capturadas por un intruso y puede llegar a obtener información que no fuera deseable.

Despedida y Cierre

Han sido tres meses hablando de cómo proteger una red Wireless y porque hay que hacerlo, así que ya no tienes excusa. Securiza tu red por tres razones.

1) Hay tecnología para hacerlo
2) No es difícil y sabes hacerlo
3) Siempre hay alguien aburrido pensando en cómo “divertirse”.