DEPARTAMENTO DE SISTEMAS INFORMÁTICOS Y COMPUTACIÓN

UNIVERSIDAD POLITÉCNICA DE VALENCIA

P.O. Box: 22012 E-46071 Valencia (SPAIN)

Informe Técnico / Technical Report

Ref. No: DSIC-II/04/05 **Pages:** 19
Title: Seguridad en Redes Inalámbricas
Author (s): Carlos de Alfonso, Miguel Caballer, Vicente Hernández
Date: 21/06/2005
Key Words: Redes, Redes Inalámbricas, WiFi, Seguridad

Introducción

Las redes inalámbricas (comúnmente denominadas *wireless*, en referencia al término inglés) suponen un aumento de posibilidades en cuanto a libertad de movimientos, facilidad de acceso, escalabilidad, etc., con respecto a las redes cableadas comunes. Permiten que podamos conectarnos a Internet desde cualquier lugar de la casa, la cama de un hotel o un salón de conferencias, sin la necesidad de recurrir a utilizar cables. Esta tecnología está basada en la emisión de señales de radio que permiten enviar datos tanto dentro como fuera de los edificios, siempre que el destino se encuentre dentro del alcance de la base.

Las ventajas de esta tecnología aumentan si consideramos que se pueden incorporar nuevos equipos a la red de una forma inmediata, sin la necesidad de tener un ni un solo cable nuevo, los inconvenientes que supone estar físicamente ligado a una conexión de red, ni tener que reorganizar la red que ya está funcionando.

Como ejemplo, una persona puede estar leyendo el correo en el aeropuerto, estar conectado al ordenador de la oficina desde un café o descargar ficheros o presentaciones de la red corporativa de la empresa, de una forma simple y rápida y sin necesidad de recurrir a ningún cable que le conecte a la red de datos.

Las redes inalámbricas suponen en la actualidad una alternativa muy versátil para la extensión, el enriquecimiento y la mejora del uso de las redes que ya se están utilizando. Sin embargo, todas estas facilidades conllevan también una serie de problemas de seguridad asociados a la flexibilidad y la escalabilidad. Por ejemplo, una persona no autorizada puede acceder de forma sencilla a la red inalámbrica, sin necesidad de tener acceso físico directo a la infraestructura. Como consecuencia, podría utilizar los recursos disponibles en la red asociada a la conexión inalámbrica. Dado que las redes inalámbricas complementan, extienden y generalizan las cableadas tradicionales, los recursos disponibles en éstas pueden igualmente ir desde el acceso a Internet, hasta documentos confidenciales.

En los siguientes apartados de este documento veremos algunas características de la tecnología wireless y esquemas básicos de redes establecidas por medio de esta tecnología. A continuación se mostrarán algunos tipos de organizaciones de redes típicas, en las que los dispositivos wireless van a ser las piezas principales. Seguidamente, se describirán algunos aspectos que van a condicionar la seguridad de la red construida por medio de dispositivos inalámbricos. Finalmente se proporcionarán unas recomendaciones que permitirán establecer unos niveles de seguridad suficientes, en función de las necesidades de la red concreta.

Definiciones

En este apartado se van a describir algunos términos que serán útiles en el resto del documento. Las definiciones incluidas en este apartado deberán ser interpretadas en el documento tal y como están aquí explicadas, ya que pueden dar lugar a confusiones debido a los distintos contextos en que pueden estar utilizados, y los distintos significados que han ido adoptando debido a la diversidad de ámbitos en que han sido aplicadas.

Wi-Fi

El término Wi-Fi hace referencia a una marca creada por la Wi-Fi Alliance. Normalmente se ha hecho coincidir el nombre WiFi con la propia tecnología Wireless, pero en realidad es el acrónimo de "Wireless Fidelity", que hace referencia al grado de compatibilidad entre distintos dispositivos Wireless.

El hecho de que un dispositivo esté certificado como WiFi quiere decir que ha pasado unas pruebas de conformidad con el estándar WiFi y por lo tanto es compatible con otros dispositivos con el mismo grado de certificación.

DHCP

Las siglas DHCP se corresponden a Dynamic Host Configuration Protocol. Este protocolo es utilizado para obtener direcciones IP, y resto de información de red necesaria (mascara de red, puerta de enlace…), de forma dinámica a través de un servidor central. Este sistema permite configurar un grupo grande de dispositivos de red de forma sencilla y transparente al usuario.

NAT

La Traducción de Direcciones de Red, o NAT (Network Address Translation), es un sistema que se utiliza para tener un grupo de direcciones privadas dentro de nuestra red, y que exteriormente sean vistas con unas direcciones IP diferentes. Usar NAT tambien permite asignar una red completa (o varias redes) a una sola dirección IP.

NAT se utiliza principalmente por dos razones:

- Seguridad: ya que permite ocultar las direcciones internas de los dispositivos al exterior de NAT.
- Escalabilidad: permite a una red tener tantas direcciones internas como sean necesarias, aunque el rango de red externo no lo permita.

DSL

Las siglas DSL (Digital Subscriber Line) agrupan a una serie de teologías de comunicación que utilizan el cableado telefónico como medio de transporte. Para ello utiliza un rango de frecuencias superior a las que utilizan las llamadas tradicionales. Existen diferentes variantes SDSL, HDSL, VDSL… entre las que destaca el ADSL por ser la más utilizada en la actualidad. Las conexiones DSL pueden llegar a alcanzar anchos de banda de 32Mbps.

IEEE

El Institute of Electrical and Electronics Engineers (IEEE) también conocido como i-e-cubo, es una organización profesional técnica sin ánimo de lucro que incluye a más de 377.000 socios en 150 países. A través de sus socios el IEEE se ha convertido en una autoridad en varias áreas técnicas, desde ingeniería informática hasta ingeniería en telecomunicaciones, pasando por otras como ingeniería biomédica o ingeniería eléctrica.

A través de su extensa red de publicaciones, conferencias y actividades destinadas al desarrollo de estándares, el IEEE produce el 30% de las publicaciones en ingeniería eléctrica e informática, y ramas afines. Actualmente lleva a cabo anualmente 300 conferencias con reconocido prestigio internacional, y patrocina el desarrollo de más de 900 estándares.

MAC

El término MAC (Media Access Control) se utiliza para referirse a la dirección física de un dispositivo de red. Esta dirección debe ser única para cada dispositivo de red y es asignado en el momento de su fabricación.

Una dirección MAC esta formada por 6 bytes que se representan en formato hexadecimal de esta forma: 11:22:33:44:55:66. De esos 6 bytes los 3 primeros corresponden con el

identificador del fabricante, y los 3 siguiente con el identificador único de cada dispositivo. El identificado del fabricante es asignado por el IEEE para asegurar su unicidad. Es responsabilidad del fabricante asegurarse la unicidad del identificador del dispositivo para evitar repeticiones.

SSID

El Service Set Identifier (SSID) es un identificado de 32 caracteres incluido en todos los paquetes transmitidos a través de una red wireless y que sirve para diferenciar a una red wireless del resto. De esta manera permite que varias redes puedan operar simultáneamente en la misma área física. El SSID es tambien llamado comúnmente como nombre de red, ya que esencialmente es, ese nombre, el que identifica a una red.

Tecnología Wireless

Las redes *wireless* se basan en las tecnologías de radio 802.11a, IEEE 802.11b y 802.11g para proporcionar una conectividad rápida, segura, confiable y sin cables. Las redes WiFi operan en las bandas de radio de 2.4 y 5 GHz, con un ancho de banda de 11 Mbps (802.11b) o 54 Mbps (802.11a y 802.11g). Existen dispositivos que son capaces de trabajar utilizando ambas bandas, de manera que se obtienen unas prestaciones similares a una conexión Ethernet del tipo 10BaseT.

De acuerdo con la forma en que se organizan las comunicaciones entre los dispositivos se pueden distinguir dos configuraciones principales: aquellos casos en que los dispositivos se conectan entre sí directamente y dan lugar a las redes denominadas "ad-hoc", y los casos en que la comunicación se canaliza a través de un punto de acceso que se encarga de realizar la distribución de la información. Esta segunda topología es la denominada como "infraestructura". En la Figura 1 se muestra un esquema básico de estas organizaciones.

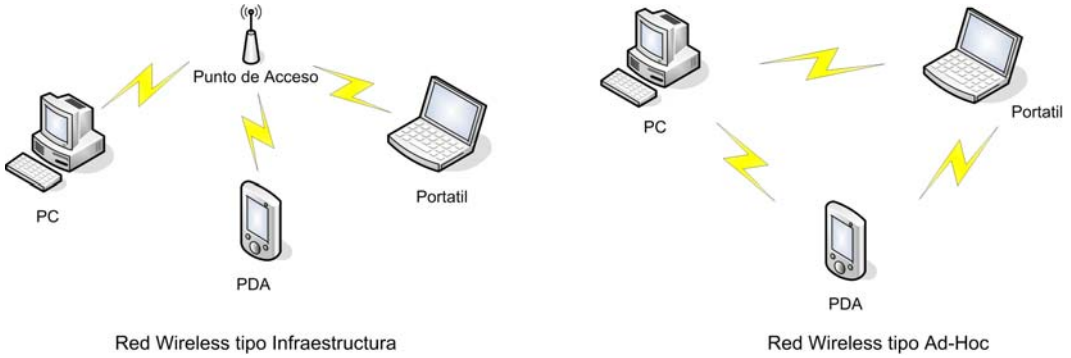

Figura 1. Tipo de redes Wireless.

El caso de las configuraciones *ad-hoc* es bastante sencillo, ya que consiste básicamente en conexiones par a par (P2P) y las precauciones de seguridad generales consisten en evitar descuidos como permitir todas las conexiones, o dejar que el sistema operativo se conecte de forma automática sin verificar la red, etc. Por lo tanto, en el resto del documento vamos a centrarnos en los aspectos de seguridad y topologías en modo infraestructura o manejado (del inglés, *managed*).

Los puntos de acceso pueden ser de dos tipos: los *puntos de acceso* básicos y los *gateway*. Los puntos de acceso básicos se encargan de conectar todos los dispositivos inalámbricos entre si y con una red cableada. En relación con las redes cableadas habituales, un punto de acceso se comporta como un *switch* de dispositivos inalámbricos, que además transmite la información a la red cableada. De este modo se consigue que todos los dispositivos pertenezcan a una misma red local utilizando un enlace transparente. El caso de los gateways es un diferente, ya que tratan a la red cableada y la inalámbrica como dos redes

separadas; de este modo el *gateway* trabaja como un router que enlaza ambas redes por medio de un elemento no transparente. Los *gateways* suelen proporcionar una serie de servicios adicionales como DHCP, NAT, VPN, etc. que son los que le confieren la entidad de elemento activo de unión y evitan la necesidad de añadir nuevos dispositivos dedicados a la red inalámbrica para realizar funciones las funciones específicas que necesita la red para su funcionamiento independiente.

Organizaciones típicas

Existen diferentes formas de configurar una red wireless y su unión con una cableada, atendiendo a distintos factores que van desde la finalidad que se le quiera dar a la red hasta el tamaño de la misma, debiendo considerar multitud de variables intermedias. A continuación vamos a describir distintas organizaciones de red sencillas, para mostrar algunas de las organizaciones típicas que se suelen considerar en para las redes sin cables.

SOHO

El objetivo de las configuraciones SOHO (Small Office and HOme) es el de utilizar la red wireless para facilitar el establecimiento de una red corporativa para una empresa de tamaño pequeño o la red domestica de un usuario. En este caso, una red inalámbrica permite añadir nuevos ordenadores de forma sencilla, al tiempo que facilita la movilidad de los empleados dentro de las instalaciones de la empresa, sin necesidad de modificar o añadir nuevo cableado.

En las configuraciones de tipo SOHO los diferentes dispositivos se conectan entre si usando uno o varios puntos de acceso y habitualmente, a través de uno de ellos, se habilita el acceso a una conexión a Internet (DSL, RDSI, Cable, etc.). De este modo, cualquier dispositivo de la red inalámbrica puede tener salida al exterior.

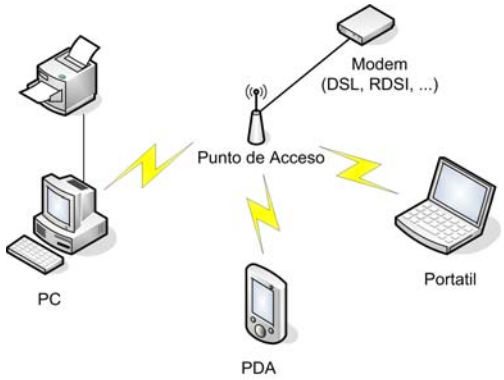

Figura 2. Organización tipo SOHO.

HotSpot

Los puntos de acceso al publico (HotSpot), se están extendiendo por cafeterías, hoteles, aeropuertos, centros de convenciones, etc. En estos lugares una red inalámbrica proporciona acceso a Internet a los clientes o a los visitantes. Para ello pueden usar sus propios equipos si tienen instalados dispositivos inalámbricos (portátiles, PDAs, etc.), o utilizar equipos proporcionados en los propios locales.

El modelo de negocio aplicado en este caso varía desde los servicios de forma gratuita (para proporcionar el servicio como un valor añadido) o pagando una cuota de acceso (bien a la red o bien por medio del alquiler del equipo). La Figura 3 muestra un esquema básico de este tipo de configuración.

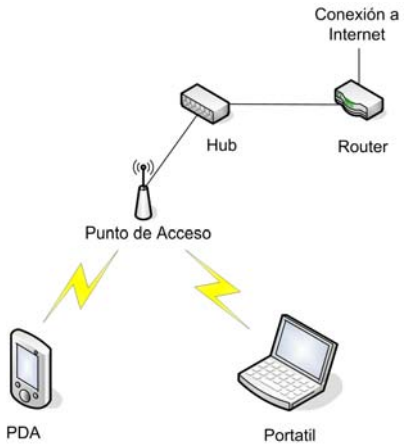

Figura 3. Organización tipo HotSpot.

La diferencia principal con respecto a la configuración SOHO es el aislamiento completo de la red inalámbrica por medio de un *router*. De este modo se puede independizar completamente la red inalámbrica de la red privada del local que la ofrece. Adicionalmente, mediante un *hub* o un *switch* se puede completar la diversidad de recursos que se ofrecen a los clientes de la red inalámbrica (impresoras, scanners, etc.), o extender la red incorporando nuevos puntos de acceso.

Combinación Wireless y Cable

El caso más frecuente en las redes que usan tecnologías wireless, es aquel en el que se combinan con una red cableada estándar. De este modo se consigue crear una red flexible y fácil de ampliar, haciendo que sea mucho más sencillo añadir nuevos equipos a red.

Principalmente se utilizan 2 orientaciones para combinar una red cableada con una inalámbrica, en función del dispositivo que se utilice para unir las dos redes.

En el caso de disponer de una red de cable ya instalada y se desee dar la posibilidad de incorporar dispositivos inalámbricos, se puede utilizar un punto de acceso conectado directamente a la red cableada. Otra posibilidad consiste en la utilización de un gateway wireless que, como se ha dicho en puntos anteriores, proporciona características adicionales, como es la posibilidad de crear una subred inalámbrica independiente de la cableada.

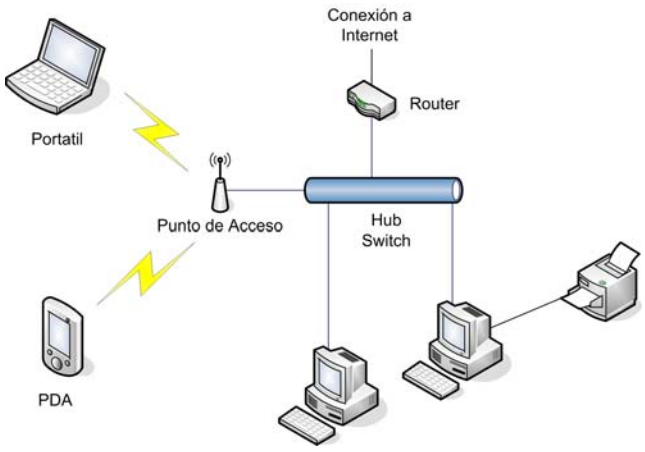

Figura 4. Combinación wireless cable.

En ambos casos se consigue el mismo resultado, que es combinar una red cableada con una wireless, de manera que unos y otros puedan conectarse entre si, de forma transparente; sin embargo, se siguen aproximaciones distintas en función de las

características de interacción que se desea proporcionar a los dispositivos de la red Inalámbrica con la cableada.

Intrusos e intrusiones

El hecho de disponer de una red abierta y de fácil acceso es muy útil en una organización o la casa del usuario doméstico. Sin embargo hace que su utilización sea muy atractiva para personas ajenas a la organización (o el particular) que la establece. Este tipo de *intrusos* puede suponer problemas para la red, por diversos motivos: desde la simple utilización del ancho de banda de la red hasta la desconfiguración de la misma, pasando por la consulta de documentos no autorizados.

Para conocer los riesgos a los que se enfrentan los usuarios y los propietarios de la red inalámbrica es importante conocer, por un lado, los motivos que llaman a la intromisión en este tipo de redes y por otro, los perfiles de estos intrusos [1].

Motivos de intrusión

Los motivos de intrusión en las redes tradicionales se escapan del objeto del presente documento; sin embargo, las redes inalámbricas introducen una serie de características que pueden suponer nuevos alicientes para la intromisión en ellos.

En los siguientes apartados se comentan los principales motivos por los que resulta atractivo para los intrusos el hecho de realizar intromisiones en este tipo de redes.

Diversión y nuevos retos

El *hacking* y *cracking* se han puesto en práctica tradicionalmente utilizando medios lógicos. Esto quiere decir que se suele tratar de realizar intrusiones utilizando programas y medios basados en la lógica de computación (programación, búsqueda de fallos en los programas y sistemas operativos, puertas traseras, etc.).

En el caso de las redes inalámbricas se involucran, además de los programas habituales, algunos agentes físicos (equipos, antenas, dispositivos de transmisión, puntos de acceso, etc.) que pueden llamar la atención a los usuarios curiosos, de modo que éstos comiencen a realizar intrusiones por el simple hecho de suponer un nuevo reto o una diversión.

Acceso casi-anónimo a la red

Para tener acceso a Internet, es necesario que se disponga de un proveedor de servicios, a través del cual se realizan los accesos pertinentes, a los recursos correspondientes. En caso de que se esté cometiendo un delito a través de este acceso a la red (por ejemplo, realizando una intrusión en una red), si se consigue identificar el proveedor de servicio desde el que se ha originado el ataque, las autoridades pueden solicitar al proveedor de servicio la identidad de la persona que ha llevado a cabo el acceso y, de acuerdo a la normativa legal, debe de disponer de ella y de proporcionársela.

Dada la regulación existente (que en muchos países obliga a los proveedores de servicios de Internet a mantener los archivos de acceso durante varios años), siguiendo métodos tradicionales, la mecánica suele consistir en ir saltando de equipo en equipo (geográficamente distribuidos y pertenecientes a distintos proveedores de servicio), de modo que se puedan diluir el rastro y al tiempo puedan ir borrando las pistas del delito (por ejemplo, eliminando los archivos de *log*) que puedan probar la culpabilidad y/o los saltos que ha hecho el intruso. El objetivo final consiste en que el rastro del delincuente sea difícil de averiguar. Sin embargo, no siempre es posible eliminar los archivos de registro de todos los equipos y esto puede suponer una trampa para el *intruso*.

En el caso en que el ataque se origina a través de una intrusión en una red inalámbrica, llega un momento en el que la pista (literalmente) se "desvanece en el aire". De este modo, un rastreo de las pistas únicamente podrá conducir al propietario de la red de la cual se está abusando. Como resulta obvio, esto supone un gran atractivo para la intrusión con fines delictivos.

Puertas traseras a las redes

Un mal diseño de una red inalámbrica, o del enlace entre la parte inalámbrica y la parte cableada de una red corporativa, pueden suponer una puerta trasera a la red privada de una organización.

Esto puede hacer que métodos de espía que estaban parcialmente extinguidos gracias al aislamiento de las redes corporativas de las redes públicas (*sniffers* de claves, transmisión no encriptada de correo y tráfico de red en general, etc.) puedan volver a ponerse en práctica por el simple hecho de que con este mal diseño se llega a "ofrecer" al público un acceso libre a la red interna.

Siguiendo una orientación recíproca, un *hacker* interesado en tener acceso a estas redes internas puede utilizar este tipo de tecnologías inalámbricas (instalando un punto de acceso o una tarjeta wireless en la red privada) para establecer una puerta trasera en el sistema y con ello, evitar los controles de acceso a la red. Una vez dentro de la red, se pueden habilitar las técnicas de *pirateo* tradicionales.

Oportunismo

Un motivo muy simple, que puede no resultar obvio a priori, es el hecho de que alguien realice una intrusión en una red "porque se puede". Esto es lo que suele ocurrir cuando un usuario pone en funcionamiento un dispositivo inalámbrico y accidentalmente encuentra redes disponibles en su entorno. En estas situaciones se pueden dar acciones casuales que tienen como resultado la utilización del ancho de banda, el espiar las páginas web que son consultadas desde el interior de la red o incluso la lectura de correos electrónicos.

Perfiles de los intrusos

Una vez conocidos los tipos de intrusiones más habituales, es importante conocer los perfiles de las personas que las llevan a cabo. Éstas pueden ser desde el informático curioso que se "encuentra" una red hasta un *hacker* experimentado que trata de hacer un ataque premeditado.

Usuarios curiosos

Este tipo de usuarios realiza las intrusiones principalmente por dos motivos: diversión y reto técnico. En realidad no suponen grandes problemas para la red ya que se limitan a descubrir redes, comprobar que pueden realizar intrusiones no destructivas, e incluso llegan a avisar al propietario de la red para que corrija sus fallos.

Utilización de ancho de banda

Este es el caso de usuarios que realizan las intrusiones para utilizar el ancho de banda de la red. En este perfil se pueden incluir las personas que utilizan las redes para navegar sin necesidad de pagar una conexión a un proveedor de servicio. Sin embargo, los que pueden resultar problemáticos son aquellos usuarios que "hurtan" este ancho de banda con el fin de transmitir contenidos problemáticos (música, pornografía, etc.). Estas personas realizan las intrusiones con el fin de obtener un ancho de banda cuasi-anónimo que les permita transmitir contenidos ilegales sin exponer su identidad, como se comentó en apartados

anteriores, ya que el rastreo de las transmisiones conducirá al usuario que está sufriendo la intrusión.

Este tipo de intrusiones es relativamente fácil de rastrear y al tiempo fácil de evitar, ya que el uso de mecanismos de protección sencillos (encriptación WEP y listas de control de acceso de direcciones MAC) suele ser suficiente para desanimar a los intrusos.

Hackers/Crackers

Estos usuarios son los que pueden suponer un problema serio para la red objetivo de sus intrusiones, ya que son gente que sabe qué es lo que está haciendo, cómo hacerlo y las implicaciones (legales) que puede tener.

Este tipo de intruso puede utilizar la red como objetivo o como simple medio de paso a otro objetivo. En el segundo caso, la intrusión en la red inalámbrica será una forma de ocultar su identidad y evitar los posibles rastreos. Sin embargo, ante la primera situación, es importante tener en cuenta que el intruso en la red se convierte en un atacante cuyo objetivo no es el compromiso de la seguridad de la red inalámbrica en sí, sino que la utiliza para acceder a alguno de los equipos que residen en la misma.

Las medidas de seguridad deben ser extremadas si se esperan este tipo de atacantes, ya que cualquier intento de seguridad simple (listas de control de acceso, encriptación WEP) únicamente va a conseguir retrasar los ataques porque están técnicamente cualificados y posiblemente dispongan de la infraestructura adecuada (antenas direccionales, transmisores potentes, etc.) para salvarlos sin muchos problemas.

Medidas de seguridad

Existen diferentes aspectos relacionados con el tema de la seguridad en las conexiones de red inalámbricas: el control de acceso de los dispositivos a la red, la seguridad en los datos que circulan a través de la misma y la seguridad de los elementos físicos.

Seguridad de los elementos físicos

En la seguridad de los elementos físicos entran aspectos como la accesibilidad física a los equipos, la intercepción de la señal, etc. En el caso de las redes físicas, se puede "pinchar" el cable para interceptar la señal, pero en el caso de las redes wireless, la señal ya está en el aire y es fácilmente interceptable.

Sin embargo, se pueden tomar algunas precauciones que consisten básicamente en que la dispersión y accesibilidad a esta señal sea lo más controlada posible. Se trata de que la señal llegue con la mayor claridad posible a todos los puntos de nuestra red, pero tratando que la señal no salga de nuestras instalaciones, o salga con la menor intensidad posible.

Para ello uno de las maneras mas sencillas consiste en poner los puntos de acceso/gateways de la red, en la parte central del edificio de manera que la cantidad de señal que salga al exterior sea lo menor posible. Un ejemplo gráfico se muestra en la Figura 5, en el caso (a) una mala colocación del punto de acceso hace que la dispersión de la señal por el exterior de la oficina sea muy grande facilitando la interceptación de la misma. En el caso (b) la antena está colocada en la parte central, de manera que la cobertura es perfecta dentro del ámbito de la oficina, pero la dispersión por el exterior, se reduce al mínimo.

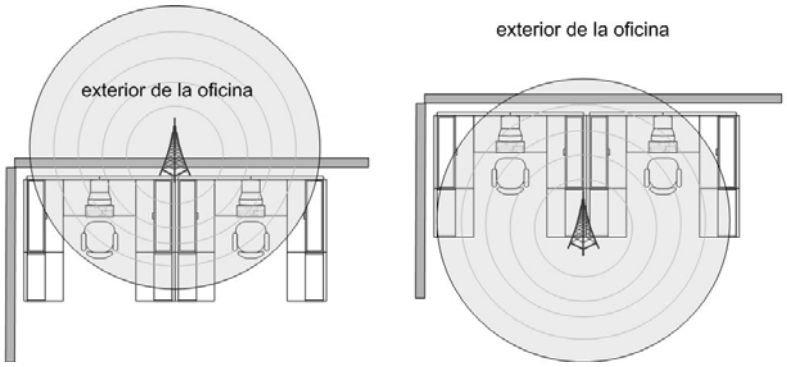

Figura 5. Colocación de puntos de acceso.

Otra posibilidad consiste en apantallar los puntos de acceso para limitar el ángulo de emisión de la señal para evitar la dispersión de la señal en todas direcciones, de manera que sea más fácil de controlar. En la Figura 6 puede verse claramente la disminución de la dispersión de la señal hacia el exterior de la oficina usando un punto de acceso apantallado (caso b) frente a un punto de acceso convencional.

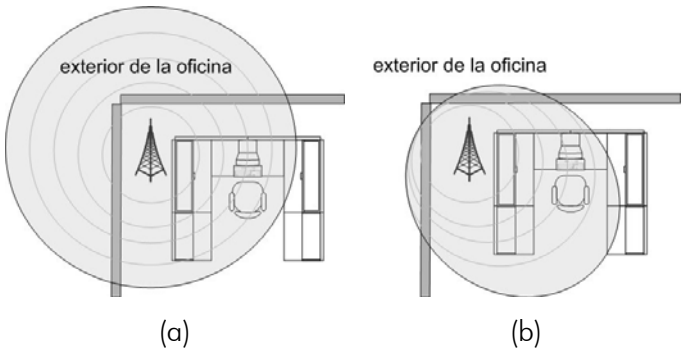

Figura 6. Puntos de acceso apantallados.

Seguridad en las comunicaciones

En la redes wireless los datos circulan a través del aire, con lo que pueden ser fácilmente interceptados sin necesidad de estar en el interior de las instalaciones de la empresa. Esto provoca un riesgo en la transmisión de datos "sensibles" a través de una red wireless. Para ello existen diferentes soluciones para evitar la interceptación de los datos. Todas ellas, de una manera o de otra, se basan en la encriptación de los datos que circulan por la red, de manera que aunque sean interceptados, no puedan ser descifrados, proporcionando, además, de manera implícita, un control de acceso a la red.

También hay que tener en cuenta los protocolos y aplicaciones que se usan a la hora de transmitir datos. Muchas aplicaciones ya utilizan sus propios sistemas de cifrado, ya que están preparadas para que esos datos puedan circular por redes públicas sin problemas de seguridad. El caso más común es el del protocolo (Secure Sokets Layer) SSL utilizado en la Web. El protocolo SSL se encarga de cifrar los documentos que circulan a través de la conexión Web. El uso de este tipo de protocolos evita la posible interceptación del contenido de los datos que circulan a través de la red, independientemente del resto de medidas de seguridad que adoptemos.

WEP

Wired Equivalent Privacy (WEP) es una técnica de encriptación de datos, que se encarga de cifrar cada uno de los paquetes 802.11 antes de su transmisión, usando el algoritmo de cifrado RC4. Este algoritmo puede usar claves de 40 a 128 bits, aumentado la seguridad usando claves de mayor tamaño. WEP no provee mecanismos para el control de claves. Todos los cambios deben hacerse de forma manual en cada dispositivo wireless.

Se ha demostrado que esta técnica tiene una serie de vulnerabilidades que permite que dicha clave pueda ser descubierta. Por esta razón actualmente se han diseñado nuevas técnicas (WPA, WPA2), que basadas en WEP, solucionan sus problemas de seguridad.

WEP es una manera sencilla de evitar el acceso no controlado a nuestra red wireless, pero es inadecuada si se requieren unas mínimas medidas de seguridad.

WPA

Wi-Fi Protected Access (WPA) aparece para solucionar las limitaciones de la seguridad proporcionada por WEP, proporcionando una compatibilidad con los dispositivos existentes. WPA es un subconjunto de la especificación IEEE 802.11i, el estándar de la seguridad en la redes Wi-Fi, y aparece como una medida intermedia hasta que el estándar 802.11i estuviera preparado (WPA aparece en Abril del 2003 y mientras que el estándar completo 802.11i fue ratificado en junio de 2004).

Las características principales son:

- Uso de el protocolo Temporal Key Integrity Protocol (TKIP) para evitar la reutilización de claves (una de las vulnerabilidades de WEP).
- Testeo de la integridad de los paquetes enviados (Message Integrity Check o MIC) para evitar errores de transmisión o manipulado de datos.

Tiene dos versiones: la personal que controla el acceso usando una contraseña denominada Pre Shared Key (PSK), y la empresarial que provee un nivel de seguridad mayor, usando claves de sesión dinámicas y verificación de usuarios usando el protocolo 802.1X EAP. Al igual que su predecesor WEP utiliza el algoritmo de cifrado RC4 usando claves de 128 bits.

WPA2

Se basa en su predecesor WPA, con las mismas características pero aumentando el nivel de seguridad, es la implementación completa de la especificación IEEE 802.11i. Una de las principales mejoras es el cambio del algoritmo de encriptado usado por WEP y WPA (el RC4) por otro más avanzado, el Advanced Encryption Standard (AES).

Como su predecesor el WPA tiene dos versiones: la personal que controla el acceso usando una contraseña denominada Pre Shared Key (PSK), y la empresarial que utiliza la verificación de usuarios usando el protocolo 802.1X EAP.

VPN

Una Virtual Private Network (VPN) es una extensión de una red privada que pasa a través de enlaces compartidos de redes públicas como Internet o una red wireless. Una VPN permite enviar datos entre dos puntos a través de una red compartida o pública de tal manera que emula una conexión punto a punto. Para emular un enlace privado los datos enviados estarán cifrados para evitar la lectura de los paquetes que puedan ser interceptados. La parte de la conexión en la que los datos circulan encapsulados es conocida como túnel.

Para la creación de estos canales seguros se utilizan una serie de protocolos como el IPsec o SSL.

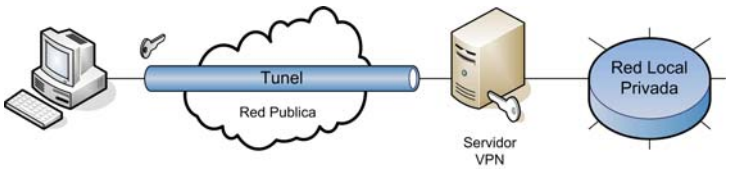

Figura 7. Conexión punto a punto de una VPN.

Desde el punto de vista del usuario la conexión VPN es una conexión punto a punto con un servidor corporativo, de manera que la naturaleza de las redes por las que circulan los datos es irrelevante.

El proceso que sigue el establecimiento de una conexión wireless a través de una VPN suele ser el siguiente:

- Al conectarse a la red wireless se obtiene automáticamente una dirección IP restringida. Con esta dirección no tenemos ningún tipo de acceso a la red local, sólo al servidor VPN.
- Conecta con el Servidor VPN y se realiza la autentificación con el nombre de usuario y contraseña.
- El servidor crear el canal de datos seguro y le asigna una IP "virtual" con acceso a la red local.

Seguridad de acceso

Con la seguridad de acceso se trata de controlar que dispositivos se conectan a nuestra red inalámbrica, de manera que evitemos posibles accesos externos no autorizados. Dependiendo del nivel de seguridad que necesitemos para nuestra red, podremos utilizar algunos de los diferentes métodos que explicaremos a continuación.

Filtrado de MAC

Cada tarjeta de red Wi-Fi tiene un identificador MAC único asignado por el fabricante (al igual que las tarjetas de red Ethernet). Este identificador puede ser utilizado por parte de los puntos de acceso, para aceptar solo a un grupo de direcciones MAC e ignorar la señal del resto.

Esta técnica puede ser un poco engorrosa para grandes empresas, con un número importante de ordenadores, ya que tendrían que dar de alta, una por una, todas las direcciones MAC de los dispositivos wireless, pero es muy efectiva para un grupo reducido de ordenadores, ya que permite tener controlado en todo momento desde que dispositivos se accede a nuestra red inalámbrica.

Además tiene el inconveniente de que existen aplicaciones de dominio público que son capaces de cambiar la dirección MAC de los dispositivos de forma ágil y eficiente. De este modo, utilizando algún medio para obtener una dirección que tenga el acceso permitido será fácil obtener acceso a la red.

EAP

El protocolo Extensible Authentication Protocol (EAP) es un protocolo de autenticación flexible, que es utilizado por el estándar IEEE 802.1X de control de acceso en las LANs. El protocolo provee a las redes wireless de un entorno para elegir un método específico de autenticación. Existen diferentes variantes del EAP:

- EAP-MD5: es la versión menos segura del protocolo EAP, utiliza el nombre de usuario y contraseña para realizar la autenticación, usando la función hash MD5 de la contraseña para la verificación. Al no comprobar la identidad del servidor es muy vulnerable a ataque del tipo *Man-in-the-Middle*.
- EAP-LEAP: es un sistema EAP propietario de Cisco. Al igual que la versión MD5, utiliza el nombre de usuario y contraseña para realizar la autenticación. Como servidor de autenticación utiliza un servidor RADIUS (explicado en apartados posteriores). Utiliza autenticación mutua pare evitar ataques *Man-in-the-Middle* como en el caso anterior.
- EAP-TLS: usa certificados X.509 tanto para el usuario como para el servidor para la autenticación mutua y el cifrado de las comunicaciones. Este sistema permite una autenticación con un nivel de seguridad muy alto, pero necesita la generación de certificados para todos los usuarios, lo cual puede ser un inconveniente para organizaciones pequeñas.
- EAP-TTLS / PEAP: en estas versiones se elimina la necesidad del certificado por parte del usuario necesario en el caso de la versión TTLS. La identidad del servidor se establece usando su certificado y la de usuario mediante un nombre de usuario y contraseña usando un servidor RADIUS.

RADIUS

El Remote Authentication Dial-In User Service (RADIUS) es un sistema de autenticación y control de usuarios usado por muchos proveedores de acceso a Internet. Actualmente RADIUS forma parte de los mecanismos de seguridad del protocolo EAP (comentado anteriormente). El servidor RADIUS es el encargado de validar el acceso de los usuarios de forma centralizada usando nombres de usuario y contraseña.

El cliente que desea conectarse a la red wireless utiliza alguna de las variantes para autentificarse. Dicha petición EAP llega al punto de acceso el cual se encargará de transmitir la petición al servidor RADIUS, el cual se encarga de validar al usuario, usando su nombre de usuario y contraseña o su certificado. El resultado de la validación es devuelto al cliente wireless, aceptando o denegando el acceso.

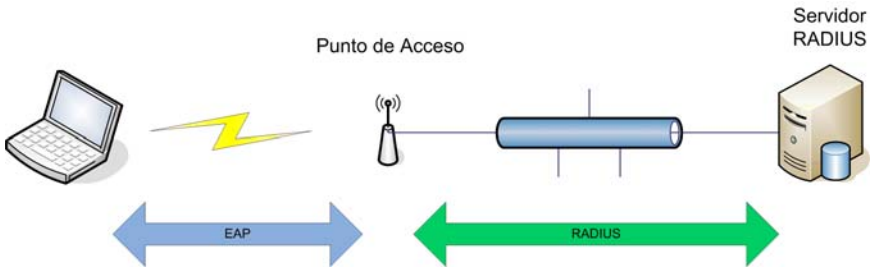

Figura 8. Autenticación EAP con RADIUS.

Algunos puntos de acceso permiten realizar filtrados de MAC usando servidores RADIUS, de manera que la MAC de la máquina que desea conectarse a la red wireless debe pasar por el servidor para ser validada.

Kerberos

Kerberos es un protocolo de seguridad desarrollado en el Instituto de Tecnología de Massachusetts (MIT), para autenticar usuarios y clientes en una red, y distribuir claves de encriptación, de forma segura. Permite que entidades que se comunican a través de una red, puedan probar su identidad, evitando que puedan ser suplantadas. Tambien

proporciona capacidades de integridad de datos (detección de modificaciones) y seguridad de datos (para evitar lecturas no autorizadas) usando sistemas criptográficos como DES.

Kerberos funcionan proporcionando a los participantes (usuarios o servicios) "tickets" digitales, que pueden usar para identificadse en la red y como clave criptográfica para hacer las comunicaciones de forma segura.

Firewalls

Los firewall o cortafuegos son dispositivos hardware o software, que funcionan como barrera entre redes, permitiendo o denegando las transmisiones de una red a la otra en función de las características de las conexiones que se pretendan establecer y las políticas de seguridad establecidas.

En este tipo de dispositivos se puede configurar el tipo de máquinas que pueden entablar conexiones con las de la red a la cual protegen, el protocolo de comunicación que pueden utilizar para ello, etc. De forma recíproca se utilizan para limitar el acceso al exterior por parte de los equipos de la red a la que protegen. En ambos casos, se definen una serie de reglas que reflejan la política de seguridad de la red.

En el caso de la redes wireless los firewalls se establecen como barrera de separación entre los dispositivos wireless y el resto de la red cableada, para evitar accesos no autorizados a zonas comprometedoras de la red, como se muestra en la Figura 9.

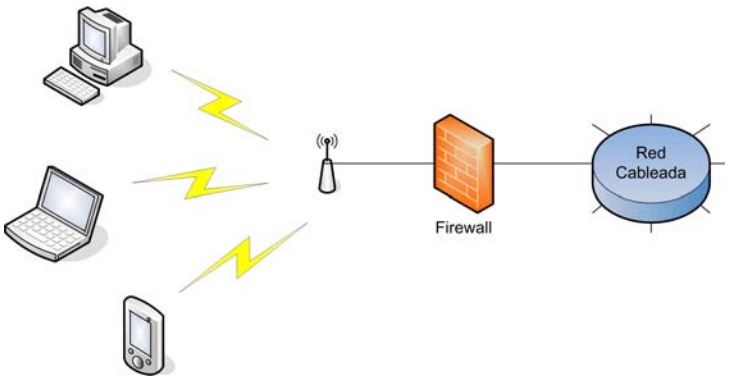

Figura 9. Uso de un firewall en una red wireless.

Algunos puntos de acceso y gateways incorporan capacidades de firewall, permitiendo crear reglas básicas que pueden ser suficientes para un entorno de red sencillo.

Recomendaciones de seguridad

Recomendaciones generales de seguridad

Independientemente del uso que se le vaya a dar a una red inalámbrica (uso privado, negocios, hotspot, etc.) es importante dotarla de unas mínimas condiciones de seguridad.

La práctica habitual del usuario individual consiste en comprar el *kit* recomendado en las tiendas, instalarlo de acuerdo a las instrucciones de "puesta en marcha rápida", y comenzar a utilizarlo lo más rápido posible. Ocurre de forma similar con las redes inalámbricas propuestas por los proveedores de servicio, que ofrecen el "*kit wifi*" para poder "usar Internet desde cualquier parte de la casa, sin cables". En estos casos, el técnico se suele limitar a instalar los dispositivos inalámbricos sin establecer una política de seguridad mínima.

A continuación se indican unas recomendaciones básicas que pueden mejorar sustancialmente la seguridad del sistema establecido.

Cambio de valores por defecto

Es importante cambiar todos los valores *sensibles* establecidos de fábrica en los dispositivos de acceso inalámbrico. Es importante seguir este paso porque, como se ha comentado en apartados anteriores, es muy fácil averiguar el fabricante de un dispositivo que disponga de una dirección MAC y a partir de la marca, obtener (a través de Internet, comprando un dispositivo similar, etc.) los manuales en los cuales están documentados todos estos valores por defecto. Entre estos valores cuyo valor se recomienda ajustar se encuentran la *clave de acceso* al sistema, el *nombre de la red* (SSID), los *rangos de direcciones*, etc.

Las recomendaciones concretas a realizar en este aspecto se enumeran a continuación:

- Cambiar el SSID de la red, estableciendo uno que no proporcione ningún tipo de pista acerca de la procedencia, la ubicación física (dirección) o cualquier tipo de dato relacionado con el particular o la empresa (nombre, teléfono, etc.) que lo ofrece. Además, es importante conseguir que el SSID sea único (que no se elija un nombre típico) para que no se convierta en una red extendida de otra ya existente por accidente (uno de los aspectos para extender una red consiste en colocar el mismo SSID en puntos de acceso distintos, y solapar la cobertura).
- Deshabilitar la publicación del SSID, para que los dispositivos de búsqueda de redes no lo detecten de forma sencilla. El hecho de que al utilizar un dispositivo estándar se revele la existencia de una red inalámbrica hace que sea muy atractivo el tratar de utilizarla. De este modo, la red pasará inadvertida para la mayoría de usuarios estándar.
- Cambio de claves por defecto, porque éstas están documentadas en numerosas páginas web, en función de los fabricantes. Esto debe ser tenido en cuenta tanto en el caso de las claves de administración de los dispositivos como en el caso de las claves de encriptación por defecto (WEP), ya que la documentación se extiende a todos los casos por defecto y no es recomendable utilizar encriptación utilizando como código aquél que ofrece el fabricante.
- Desactivación de administración inalámbrica, para evitar que alguien pueda cambiar los parámetros de configuración de acceso a la red. Muchos de los *routers* mixtos (cableado/inalámbrico) permiten seleccionar desde qué parte de la red se puede establecer la configuración del equipo. Si bien hay usuarios que no disponen de una tarjeta de red cableada para conectar por medio de cable con el punto de acceso, conviene que se considere seriamente esta medida de seguridad ya que evitará que alguien sin acceso físico al dispositivo pueda cambiar la clave de acceso al mismo, facilitar su acceso, o cambiar las opciones seleccionadas por el propietario.

Utilización de encriptación

Se ha demostrado que la encriptación WEP es vulnerable, puesto que interceptando suficientes paquetes de información se puede averiguar la clave utilizada para codificar[1]. También se ha descubierto que la encriptación WPA (sucesora de la WEP) no es del todo segura si la clave para cifrar se ha generado a partir de una palabra clave que no sea

[1] La técnica de averiguar la clave WEP no es una ciencia exacta y se basa en que algunos de los paquetes que se envían son "débiles" e incluyen parte de la clave utilizada para cifrar la comunicación. Por ello, se debe tener una suerte extraordinaria para que con muy pocos paquetes de información (~100.000) se pueda averiguar la clave. En muchos casos, incluso habiendo interceptado millones de paquetes de información no se puede averiguar la clave WEP.

suficientemente fuerte[2]. Sin embargo, utilizar WEP o WPA suele ser suficiente para repeler a muchos de los intrusos menos experimentados. En cualquier caso, el hecho de utilizar este tipo de encriptación es un primer paso y conceptualmente resulta equivalente a cerrar una puerta que en otro caso estaría abierta.

Al utilizar cualquier tipo de encriptación se debe manejar las mejores claves posibles (128 bits o superiores), y no asumir como suficientes las claves débiles de 64 bits utilizadas tradicionalmente para WEP.

En el caso en que estas claves de 128 bits se generen a partir de una palabra clave de usuario, es conveniente que sea lo más "fuerte" posible (combinando mayúsculas y minúsculas con números y signos de puntuación). Y en cualquier caso, es importante huir de casos como el de utilizar la misma palabra que el SSID de la red, o el nombre del propietario, etc.

Protección de la red

Siempre que sea posible es conveniente proteger el acceso a la red cableada desde la parte inalámbrica, aunque sea de forma simple y de acuerdo a las posibilidades del equipo que se utilice para establecer el enlace.

Restricción de puertos de acceso a la red

Es conveniente restringir las conexiones de red que puedan no tener demasiado sentido desde la red inalámbrica. En este sentido es conveniente bloquear el puerto SMTP para evitar el establecimiento de servidores de correo a través de la red inalámbrica, igual que los puertos 20, 21 y 23 para evitar conexiones FTP y TELNET y obligar a utilizar sus variantes seguras (SFTP y SSH), y aquellos utilizados por aplicaciones de intercambios de archivos P2P para evitar usos fraudulentos. Por otro lado, se pueden habilitar puertos como el 80 (para HTTP), o el 110 (para correo POP).

En cualquier caso, la recomendación general en este caso, de cara a mantener la seguridad de una red, consiste en tener cerrados todos los puertos e ir abriendo aquellos que sean necesarios y no interfieran en la seguridad de la red.

Control de acceso a la red

Siempre que el punto de acceso (o router) lo permita, es conveniente utilizar listas de control de acceso (ACL). Utilizando esta técnica se consigue que únicamente se consideren las comunicaciones que partan o estén dirigidas a aquellos equipos que tengan una dirección MAC censada y explicitada en esta lista.

Esta no es una técnica totalmente disuasoria, puesto que es relativamente fácil de burlar; sin embargo, si que evitará la mayoría de las intrusiones casuales que buscan obtener un acceso a Internet gratuito.

Del mismo modo, se debe deshabilitar la asignación automática de direcciones IPs (DHCP) si el conjunto de máquinas que vayan a acceder a la red es estable y bien conocido. En este caso es conveniente utilizar direcciones IP estáticas, configuradas manualmente en la máquina y asociadas a las direcciones MAC (si es posible, de acuerdo a las ACL). En el caso de usar IP estáticas se deben evitar usar direcciones de red bien conocidas como son las 192.168.0.* o 10.0.0.*.

---

[2] Para facilitar la generación de una clave de 128 es habitual que se utilice un algoritmo de que, a partir de un texto genera dicha clave.

En caso de que no se den las condiciones que permitan prescindir del protocolo DHCP, es conveniente limitar al máximo el rango de direcciones que van a poder ser asignadas de forma automática. De este modo se estrechará la horquilla de posibles máquinas que puedan acceder a la red de forma simultánea[3].

Diagnóstico de la red

Independientemente de las técnicas que se utilicen para proteger la red, es conveniente realizar un diagnóstico periódico a la misma con el fin de consultar los posibles accesos establecidos, las operaciones realizadas, etc. Es importante prestar acceso a los ficheros de seguimiento (logs) ya que en éstos es posible que se expliciten posibles errores (máquinas distintas con IPs idénticas, intentos de accesos no autorizados, máquinas con IPs iguales y direcciones MAC distintas, etc.).

Recomendaciones de seguridad avanzadas

Además de las recomendaciones indicadas en el apartado anterior, en caso de que la red inalámbrica vaya a ser utilizada en un ámbito empresarial con utilización de contenidos confidenciales, es importante considerar algunos aspectos adicionales.

Aislamiento de la red inalámbrica

Es conveniente aislar totalmente la parte inalámbrica de la parte cableada de la red, utilizando firewalls que establezcan unas reglas adecuadas para permitir la unión de una forma segura.

En este sentido, el firewall gestionará tanto los accesos desde la red inalámbrica a la cableada (aplicando políticas de seguridad adecuadas), como los recíprocos (de la cableada a la inalámbrica). De este modo se evitarán las consideraciones de seguridad por omisión.

Utilización de encriptación

En el caso de uso empresarial, la encriptación base utilizada debe ser WPA con códigos de fuerza igual o superior a 128 bits. Además deberemos tratar de utilizar palabras claves fuertes (mayúsculas y minúsculas combinadas con números y signos) para generar estos códigos utilizando los algoritmos de hash proporcionados por los fabricantes[4]. De todos modos, será conveniente actualizar el *firmware* de los dispositivos para que eviten utilizar paquetes débiles a partir de los cuales se puedan lanzar ataques.

A pesar de que la encriptación WPA es razonablemente buena si se utiliza bien (claves "fuertes"), es mejor basar las comunicación en WPA-2, si está disponible.

Independientemente de la codificación que se aplique a la señal, en el caso corporativo es altamente recomendable utilizar métodos de encriptación avanzados, como puede ser la creación de VPNs o la utilización de protocolos seguros como SSL para la copia de ficheros, envío de información sensible, etc.

---

[3] Si la organización sólo tiene 15 equipos no tiene sentido tener 200 IPs disponibles para ser asignadas vía DHCP.

[4] De este modo se evitarán los ataques de diccionario contra la encriptación WPA.

Protección física de la red

En el caso de que se vaya a dar un uso corporativo a la red inalámbrica, será conveniente proteger "físicamente" la red para que únicamente acceda el personal autorizado. Para ello, las recomendaciones consistirán en las siguientes:

- Hacer un estudio de cobertura para detectar la mejor ubicación de los puntos de acceso y routers inalámbricos, de forma que la señal no cubra zonas ocultas o desprotegidas. De este modo se trata de evitar que una persona pueda acceder a la red de la organización desde fuera del espacio físico de la misma.
- Realización de escaneos de red periódicos, con el fin de detectar puntos de acceso no autorizados, o equipos que están ejerciendo de intrusos.

Protección lógica de la red

La protección lógica de la red hace referencia a aquellas técnicas que se van a aplicar utilizando aplicaciones y protocolos de comunicaciones. Las siguientes recomendaciones deben complementar a las generales propuestas en el apartado anterior.

- En este caso es imprescindible mantener cualquier puerto TCP/UDP cerrado por defecto para las redes inalámbricas. En caso necesario, se deberá estudiar la apertura de cada puerto individual, con el fin de determinar las implicaciones que puede tener su liberación. En caso de que sea posible, se deberá también acotar la apertura de un determinado puerto a las máquinas que vayan a hacer uso explícito del mismo.

  Como recomendación general, debe imponerse (a nivel corporativo) el uso de protocolos seguros como SSH, SFTP o HTTPS en lugar de TELNET, FTP o HTTP. Por el mismo motivo, se deberá evitar la apertura de puertos susceptibles de ser atacados, como los utilizados por las aplicaciones de intercambio de ficheros.
- Comprobar los archivos de seguimiento (logs), con el fin de detectar comportamientos anómalos de la red, solicitudes DHCP no autorizadas, etc.
- Limitación de las máscaras de red para, junto con la limitación de la horquilla de direcciones IP a proporcionar en el caso de utilizar el protocolo DHCP, conseguir una red cerrada.
- Mantenimiento al día de las ACLs para evitar que equipos que ya no van a acceder a la red inalámbrica tengan la posibilidad de utilizarla. De este modo se consigue evitar que un intruso que conozca una dirección MAC autorizada que ya no está siendo utilizando pueda continuar con su acceso.
- Limitar el acceso a direcciones desde la parte inalámbrica de la red, de modo que únicamente se pueda acceder a determinados equipos de la red cableada. Este método puede ser disuasorio para intrusos que busquen ancho de banda gratuito.
- Utilización de servidores de autenticación de usuarios, como por ejemplo RADIUS o NoCat. En estos casos se debe restringir el acceso a la red hasta que el usuario no se haya autenticado adecuadamente.

Políticas de seguridad integradas

El método más eficaz de mantener protegida una red al incorporarle una vertiente inalámbrica consiste en crear una política integrada de seguridad para la parte cableada y la inalámbrica.

En esta política debe considerar el tipo de información que va a ser protegida, si puede ser accesible desde el exterior, si puede ser accedida desde la parte cableada y/o la inalámbrica de la red, etc. Así mismo se deberán considerar los protocolos de comunicaciones que se van a permitir desde y hacia cada una de las partes de la red (privada cableada, privada inalámbrica o pública).

Se deberán contemplar normativas de seguridad con respecto a los recursos compartidos (impresoras, espacio en disco, etc.), así como en aspectos referentes al mantenimiento de claves, certificados, direcciones, etc. que permitan el acceso a los mismos.

En definitiva, la parte inalámbrica de la red debe ser considerada dentro de la política de seguridad de la red en conjunto, y no debe ser únicamente vista como un nuevo medio de acceso.

Condiciones de seguridad establecidas

Las condiciones de seguridad que se están implantando en los despliegues que se realizan en la actualidad en los ayuntamientos que se encuentran dentro del Plan Provincial de Acceso a Internet (PAI) aportan un elevado nivel de seguridad, al tiempo que llegan a un compromiso de facilidad de uso y crecimiento.

En concreto, las medidas de seguridad establecidas siguen prácticamente la totalidad de las recomendaciones generales de seguridad, e incorporan alguna de las recomendaciones de seguridad avanzadas.

Estas medidas de seguridad comienzan por el cambio de la mayoría de los valores por defecto de los puntos de acceso, para evitar las intrusiones destructivas documentadas en Internet. Estas suponen la gran mayoría de los problemas puesto que, como se ha comentado a lo largo del presente documento, en esta documentación se incluyen nombres de redes habituales, claves por defecto, etc. que pueden proporcionar acceso no solo a la red, sino también a la configuración y administración de la misma.

La difusión del nombre SSID de la red desplegada está desactivada en los puntos de acceso, para evitar que sea visible al resto de dispositivos inalámbricos. Por otro lado, este nombre SSID se establece de acuerdo a palabras complejas que son resultado de la combinación de letras mayúsculas y minúsculas, que no responden a palabras con sentido real. Esto evitará gran parte de los posibles ataques de diccionario[5] que se utilicen para tratar de descubrir si hay alguna red inalámbrica instalada.

Adicionalmente, la red está protegida por una encriptación basada en clave WEP de 128 bits, puesto que los dispositivos se encuentran actualizados con las últimas versiones de los algoritmos de encriptación, que evitan las vulnerabilidades de este protocolo. Por otro lado, la clave WEP utilizada está generada a partir de una palabra construida como resultado de la combinación de letras mayúsculas, minúsculas y números, con el fin de evitar ataques de diccionario.

Por otro lado, los puntos de acceso tienen restringido el acceso por direcciones MAC de los dispositivos autorizados. Esto quiere decir que para que un equipo tenga acceso a la red inalámbrica deberá de haber sido dado de alta en los puntos de acceso correspondientes, por parte del administrador.

---

[5] Un "ataque de diccionario" consiste en utilizar palabras de una lista amplia (o diccionario) para probar a ver si ha sido utilizada como palabra clave. Este ataque es bastante simple, pero resulta efectivo en muchos casos ya que la gente suele utilizar palabras con sentido para que les resulten fáciles de recordar, como claves de usuario, correo, etc.

Para facilitar la tarea del administrador de red local al ayuntamiento, en cuanto a alta de direcciones MAC autorizadas a acceder a la red, y solucionar problemas puntuales dependientes de la configuración, se ha dejado habilitada la administración del punto de acceso vía http.

Para que un nuevo equipo pueda acceder a la red, deberá comunicar la dirección MAC al administrador de la red, y éste deberá darla de alta en los puntos de acceso correspondiente. A continuación, deberá comunicar el nombre SSID de la red para que pueda ser visible para el usuario. Finalmente, deberá incorporar los parámetros de seguridad adecuados, que permitan el diálogo correcto con los puntos de acceso.

Bibliografía

[1] Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky, "Wi-Foo: The Secrets of Wireless Hacking". Addison Wesley, Junio 2004.

[2] The Wi-Fi Alliance Index, The Wi-Fi Alliance [online] 2004, http://www.wi-fi.org (accedido: 15 de Febrero de 2005).