ISEC Lab #6

Análisis de redes wireless

Parte 2
Medidas de seguridad

Vicente Aguilera Díaz
vaguilera<arroba>isecauditors.com

1 INTRODUCCIÓN 3

2 MEDIDAS DE SEGURIDAD 4

2.1 MEDIDAS DE SEGURIDAD PREVENTIVAS 5
2.1.1 ADOPCIÓN DEL ESTÁNDAR 802.11I 5
2.1.2 USO DE VPNS 6
2.1.3 QOS 8
2.1.4 DESHABILITAR BROADCAST DE SSID 9
2.1.5 DESHABILITAR DHCP 9
2.1.6 REALIZAR FILTRADO POR MAC 10
2.1.7 CAMBIAR DATOS SENSIBLES POR DEFECTO 10
2.1.8 CONTROLAR EL PODER DE LA SEÑAL 10
2.1.9 MANTENERSE INFORMADO SOBRE ACTUALIZACIONES 11
2.1.10 UTILIZAR CIFRADO FUERTE 11
2.1.11 CREAR UN SEGMENTO DE RED DEDICADO 11
2.1.12 REVISAR PERIÓDICAMENTE LA SEGURIDAD DE LA RED 12
2.2 MEDIDAS DE SEGURIDAD DETECTIVAS 12
2.2.1 MONITORIZACIÓN DE LA RED 12
2.2.2 HABILITAR EL LOGGING EN LOS DISPOSITIVOS 12

3 CONCLUSIONES Y RECOMENDACIONES 14

4 ENLACES DE INTERÉS 15

5 GLOSARIO 16

1 Introducción

Habíamos comentado en la primera parte (ISEC Lab #5: "Herramientas y técnicas de ataque") de este artículo algunas de las deficiencias y vulnerabilidades que sufren las redes wireless así como las técnicas más empleadas para explotar dichos problemas.

Esta segunda parte del artículo pretende abordar la seguridad de este tipo de redes desde el punto de vista del administrador, aportando soluciones a los problemas anteriormente planteados.

Finalmente, en el apartado Conclusiones y Recomendaciones se ofrece un resumen final de la situación en la que se encuentran las redes wireless desde el punto de vista de la seguridad, a partir de los aspectos comentados en este ISEC Lab.

2 Medidas de seguridad

En el anterior ISECLab comentamos ciertas medidas de seguridad de carácter básico que podíamos adoptar en las redes wireless, pero que resultaban insuficientes tal y como vimos al llevar a cabo los siguientes ataques:

- Obtención de claves WEP
- Evasión del filtrado por MAC
- Obtención de SSIDs ocultos
- DoS

En esta ocasión intentaremos avanzar un poco más en cuanto a la protección tanto de la red como de la información que transmitimos. De esta forma, conseguiremos evitar, o cuando menos paliar, los problemas anteriormente enumerados.

A la hora de adoptar medidas de seguridad, estaremos hablando básicamente de dos tipos:

- **Medidas de seguridad preventivas**: englobaríamos en esta categoría todas aquellas medidas cuya finalidad es la prevención de los problemas relacionados con la seguridad de la red.
- **Medidas de seguridad detectivas**: hacen referencia a todas aquellas medidas que podamos adoptar con la intención de detectar problemas de seguridad que se hayan producido en la red.

Veamos a continuación qué medidas podemos adoptar y en qué consisten.

2.1 Medidas de seguridad preventivas

En cuanto a las medidas que podemos adoptar con la intención de prevenir problemas de seguridad en nuestra red wireless, podemos destacar las siguientes:

2.1.1 Adopción del estándar 802.11i

Una de las principales deficiencias que habíamos comentado en la primera parte de este artículo era el propio estándar WEP. Por supuesto, este hecho era conocido por todos, por lo que no tardaron en surgir alternativas que incorporaban nuevas mejoras.

El estándar 802.11i surge tras la evolución de WEP, corrigiendo sus deficiencias tras pasar por varios estadios (WEP2, WAP, WAP2).

En la siguiente tabla se observa esta evolución:

		ESTÁNDARES				
		WEP		WPA		802.11i
CARACTERÍSTICAS	Algoritmo cifrado	RC4	WEP2	RC4	WPA2	AES
	Tipo de cifrado	Flujo		Flujo		Bloque
	Protocolo de seguridad	-		TKIP		CCMP
	Distribución de claves	Manual		EAP		EAP
	Comprobación integridad	CRC32		TKIP(Michael)		CCM
	Año aparición	1999		2002		2004

Como se puede apreciar, la evolución de WEP nos ha llevado al estándar 802.11i (estándar de seguridad en redes wireless), ratificado en junio de 2004 por el IEEE.

Proporciona encriptación fuerte, autenticación y estrategias de gestión de claves.

802.11i define dos protocolos para la seguridad en la transferencia de los datos: TKIP y CCMP. De esta forma, la adopción del estándar 802.11i garantiza que:

- Nunca se envían o reciben paquetes no protegidos
- Autenticidad en el origen del mensaje (previene falsificaciones)
- Paquetes con número de secuencia (detecta reenvíos)
- Protección de la dirección origen y destino
- Confidencialidad e integridad mediante el uso de técnicas de cifrado fuerte

TKIP puede ser utilizado para enmascarar las debilidades de WEP (falsificación de datos, ataques de repetición, cifrado y reutilización de claves) manteniendo el mismo hardware y sólo actualizando el software/firmware, sin degradar excesivamente el rendimiento.

TKIP proporciona las siguientes mejoras:

- Combinación de clave por paquete: generando una clave distinta para cada paquete.

- IV (Initialization Vector) de 48 bits: En WEP sólo se utilizaban 24 bits.

- MIC (Message Integrity Check): Se descartan todos los mensajes que no hayan sido validados. De esta forma se evitan los ataques conocidos como man-in-the-middle.

CCMP es una solución a largo plazo. Se encuentra basado en AES en modo CCM (Counter Mode Encryption with CBC-MAC Data Origin Authenticity). El algoritmo AES requiere un uso intensivo de CPU para llevar a cabo las tareas de cifrado/descifrado, por lo que puede ser necesario la incorporación de nuevo hardware que permita acelerar este proceso.

El estándar 802.11i propone a su vez al estándar 802.1X como mecanismo de autenticación. 802.1X es la norma propuesta por el IEEE para autenticar de forma centralizada a usuarios y estaciones, y se basa en el protocolo de autenticación EAP (Extensible Authentication Protocol). Los mensajes EAP son encapsulados en mensajes 802.1X, por lo que se conocen como EAP over LAN.

802.1X es lo suficientemente flexible como para soportar distintos protocolos de autenticación, y se compone de tres elementos clave:

- **Solicitante**: el dispositivo wireless del cliente. En primer lugar se asocia y después se autentica sobre un autenticador.
- **Autenticador**: el AP (punto de acceso) que exige autenticación antes de permitir el acceso a los servicios que se suministran a través de él.
- **Servidor de autenticación**: generalmente, un servidor RADIUS. Este servidor comprueba los credenciales del solicitante en nombre del autenticador y después le responde a éste indicándole si el solicitante tiene o no permiso para acceder a los servicios que proporciona el autenticador.

2.1.2 Uso de VPNs

Las VPNs no forman parte de ningún estándar WiFi, pero es una tecnología madura que puede considerarse como una medida adicional que garantizará la privacidad de nuestras comunicaciones, y que viene siendo cada vez más empleada en la seguridad de las WLAN.

El hecho de que el estándar 802.11i no se encuentre aún lo suficientemente extendido hace que el uso de VPNs se convierta en una buena solución para la protección de nuestras comunicaciones wireless.

Las VPNs pueden implementarse en las WLAN de forma similar a como son utilizadas para proporcionar acceso remoto seguro a redes corporativas a través de Internet. La idea es convertir redes públicas (como se pueden considerar las redes wireless) en redes privadas (redes internas, seguras).

Las VPNs incorporan:

- Autenticación fuerte
- Integridad y confidencialidad de la información: Al transmitirse la información por un canal cifrado, la captura del tráfico por parte de un intruso ya no supone ningún problema.

Al hablar de implementaciones de VPNs podemos encontrarnos con tres escenarios distintos: conexión entre dos dispositivos, conexión entre dos redes o conexión entre un dispositivo y una red.

Para introducir una VPN en nuestra red wireless será necesario instalar un cliente (software) de VPN en cada una de las estaciones y usar el AP como terminador de VPN (si dispone de servidor VPN integrado) o bien utilizar un servidor VPN externo.

A continuación se enumeran las principales ventajas e inconvenientes del uso de esta tecnología en las WLAN:

Como **ventajas**:

- Usuarios familiarizados con la solución: la madurez y confianza de esta tecnología ha provocado un uso extendido de la misma, lo que ha permitido que los usuarios se sientan familiarizados y cómodos con el uso de esta solución.

- Bajo coste: la tecnología VPN no depende del hardware WLAN implantado (AP, tarjetas inalámbricas, ...), de tal forma que no es necesario invertir en nuevo hardware a pesar de que las soluciones WLAN sigan su evolución.

- Autenticación: sólo usuarios que dispongan de las credenciales necesarias podrán autenticarse contra el terminador de VPN, por lo que un intruso no podrá inmiscuirse en las comunicaciones privadas.

- Confidencialidad de la información: la solución VPN fue pensada para aportar protección de los datos al atravesar redes inseguras. Las creación del túnel VPN garantiza la privacidad de la información de extremo a extremo, por lo que un intruso que consiguiera interceptar las comunicaciones en el túnel no conseguiría obtener la información “en claro”, sino únicamente datos cifrados.

Como **inconvenientes**:

- Su uso no es transparente de cara al usuario: los clientes VPN necesitan que el usuario inicie la sesión manualmente. Además, si se produce una desconexión debido a una pérdida de potencia en la señal de la WLAN, o debido a un desplazamiento entre celdas (que implicaría la asociación a un nuevo AP), el cliente deberá volver a conectarse manualmente.

- Imposibilidad de administración remota de equipos: hasta que un usuario no haya iniciado sesión en la VPN, el equipo no será accesible y, por lo tanto, no se podrá supervisar o administrar. De esta forma, los equipos inactivos (en los que el usuario no haya iniciado sesión) o desconectados no podrán ser administrados.

- Rendimiento: uno de los problemas que se producen al incorporar algoritmos fuertes de cifrado (como habíamos comentado en el caso de AES) es el consumo intensivo de CPU en los equipos que han de realizar la tarea de cifrado/descifrado. Este hecho es especialmente grave en routers y terminadores de VPN cuando han de analizar tráfico proveniente de un gran número de clientes, convirtiendo el terminador de VPN en un cuello de botella y afectando de forma negativa al rendimiento de la red.

- Seguridad de la red: a pesar de que la VPN protege la información que se transmite por el túnel creado, esto no evita que un usuario pueda seguir intentado detectar dispositivos de la WLAN y atacarlos, por lo que esta tecnología no ofrece protección sobre la WLAN.

En cuanto a las soluciones open-source existentes actualmente y que nos permiten la creación de túneles VPN podemos destacar las siguientes:

- OpenVPN (http://openvpn.net)
- FreeS/WAN (http://freeswan.org)

2.1.3 QoS

Inicialmente el grupo encargado de diseñar 802.11i tenía como objetivo trabajar en QoS y seguridad. No obstante, rápidamente se optó por tratar dichos ámbitos de forma específica en dos estándares distintos, por lo que 802.11i se dedicó exclusivamente a tratar la seguridad y 802.11e se dedicó a QoS.

La idea en la que se basa 802.11e es simple: asignar niveles de prioridad tanto al tipo de tráfico como a los usuarios, de forma que el tráfico de la red se gestione de forma más eficaz (por ejemplo, asignar más prioridad a paquetes de voz que a paquetes de datos, asignar un nivel de prioridad superior a aquellos usuarios que hagan uso de aplicaciones a tiempo real, etc.).

Además de mejorar la calidad del servicio ofrecido por nuestra red, algo crítico en WMM (Wi-Fi multimedia) y aplicaciones como voz sobre IP, la

incorporación de este estándar nos permitirá evitar determinados tipos de ataques de DoS (Denial of Service) sobre nuestra red.

2.1.4 Deshabilitar broadcast de SSID

Muchos APs y routers wireless emiten de forma periódica el nombre de la red (SSID, Service Set Identifier) en broadcast a través de los conocidos "Beacon frames".

El nombre del SSID que se haya configurado en el AP (o conjunto de APs) debe conocerlo también la tarjeta de red del dispositivo cliente para que pueda asociarse con el AP y, de esta forma, pueda proceder con la transmisión y recepción de datos en la red wireless.

Habíamos visto, en la primera parte de este ISEC Lab, como un intruso puede obtener el SSID de una red incluso aunque los APs no lo emitan en broadcast (recordemos: monitorización del tráfico esperando la asociación de un nuevo cliente, o provocando la reasociación de un cliente con el AP).

Aún así, deshabilitar el anuncio del SSID en broadcast es una medida de seguridad que deberíamos adoptar (¿porqué facilitar la labor de un intruso?).

2.1.5 Deshabilitar DHCP

Si un intruso desea incorporarse a nuestra red (por ejemplo para utilizar con fines maliciosos nuestra conexión a Internet), deberá conocer los parámetros de la red (direccionamiento IP, máscara de red y dirección IP del gateway).

Si tenemos habilitado DHCP en nuestra red, el intruso lo tiene muy fácil ya que la información que necesita para incorporarse a nuestra red se le asigna de forma automática (en el caso de Windows, simplemente deberá activar en su interfaz de red wireless la opción "Obtener una dirección IP automáticamente").

Si deshabilitamos el servicio DHCP en la red, añadiremos una dificultad más a la tarea de un posible intruso. Debemos ser conscientes, que esta medida de seguridad no evita que los parámetros de red comentados puedan ser obtenidos por personal ajeno a nuestra red. Esta información viaja en los paquetes que se transmiten en las comunicaciones de la red wireless, por lo que si un intruso consigue acceso al tráfico "en claro" (bien porque no utilicemos cifrado, o bien porque el intruso ha conseguido descifrarlo) de un cliente de la red, podrá obtener esta información.

Aún así, es una medida de seguridad más que deberíamos adoptar.

2.1.6 Realizar filtrado por MAC

Otra medida adicional que ayudaría a mejorar la seguridad de nuestra red es la de filtrar los clientes que pueden disponer de acceso a la red. Este filtrado puede llevarse a cabo configurando ACLs (Access Control List) en los APs que especifiquen qué direcciones MAC pueden conectarse a nuestra red.

Como ocurre con otras medidas, no evita que un intruso pueda suplantar la dirección MAC de un cliente legítimo de la red (recordemos que la dirección MAC se transmite en claro, por lo que simplemente capturando el tráfico de la red es posible obtener las direcciones MAC de los clientes válidos).

Pero nuevamente, nuestro objetivo es complicar la labor de los intrusos por lo que también deberíamos adoptar esta medida de seguridad.

2.1.7 Cambiar datos sensibles por defecto

Existen parámetros sensibles (SSID, usuario y contraseña del administración del AP, etc.) en nuestra red que son conocidos de forma pública, por lo que debemos modificarlos si no queremos ver nuestra red comprometida.

Cada fabricante utiliza el mismo usuario y contraseña por defecto para sus productos, por lo que estos datos son ampliamente conocidos. Por ejemplo, un intruso que consiga conectarse a nuestra red e identifique un AP, podría acceder a la interfaz web de administración del mismo. Si nuestro AP es un C54APT (Conceptronic), el intruso conocerá que el usuario de administración por defecto es “admin” y su contraseña por defecto está en blanco. Una vez haya conseguido acceso de administrador al AP, podría modificar con total libertad la configuración del mismo (añadir su dirección MAC a la MAC Address Control List, activar la emisión del SSID en broadcast, eliminar el cifrado de la red wireless, etc.).

Otro parámetro sensible es el SSID. Por defecto nos solemos encontrar nombres del tipo “default”, “wireless”, “3com”, “linksys”, etc., por lo que también conviene modificar el SSID utilizando algún nombre complejo que resulte difícil de predecir.

2.1.8 Controlar el poder de la señal

Resulta difícil controlar que la señal wifi no sobrepase los límites deseados. Incluso cuando parece que lo hayamos conseguido, existe la posibilidad de que un intruso pueda conectarse a la red utilizando algún tipo de antena, incluso casera (recordemos, las antenas creadas a partir de botes pringles o botes de aceitunas por citar dos ejemplos).

No obstante, nuestro objetivo debe ser ajustar lo máximo posible el poder de la señal de los AP al área deseada de transmisión.

Si es posible, conviene utilizar materiales atenuantes en el perímetro de las instalaciones con el fin de debilitar al máximo la señal emitida al exterior.

A continuación se enumeran medidas de protección que nos ayudan a aumentar el nivel de seguridad en este apartado:

- Cobertura metálica en las paredes
- Vidrio aislante térmico (atenúa las señales de radiofrecuencia)
- Persianas venecianas de metal (en lugar de plásticas)
- Ubicar los dispositivos WLAN alejados de las paredes exteriores
- Utilizar pintura metálica
- Limitar el poder de la señal de los APs

2.1.9 Mantenerse informado sobre actualizaciones

Al igual que ocurre con los sistemas de las redes cableadas, dentro de nuestras responsabilidades recae el hecho de mantenernos informados ante posibles vulnerabilidades y actualizaciones que puedan sufrir nuestros dispositivos WLAN.

Para ello conviene visitar foros de confianza (en busca de vulnerabilidades detectadas y soluciones), así como las propias webs de los fabricantes con el fin de validar si existen actualizaciones de firmware para el AP o los clientes wireless.

2.1.10 Utilizar cifrado fuerte

En la primera parte de este ISEC Lab habíamos visto como el cifrado que ofrece WEP no resulta, ni mucho menos, suficiente para garantizar la protección de nuestras transmisiones wireless.

Debemos utilizar un cifrado fuerte:

- A nivel de las aplicaciones que se utilicen sobre la red wireless (por ejemplo, SSH y TLS/HTTPs)
- A nivel de tráfico wireless (por ejemplo, utilizando VPNs)

2.1.11 Crear un segmento de red dedicado

Otra medida de seguridad consiste en crear un segmento de red dedicado para la red wireless y tomar medidas para restringir el acceso a este segmento.

De esta forma aislamos los dispositivos inalámbricos de nuestra red cableada, por lo que si un intruso consigue acceso a la WLAN no significará que automáticamente dispone de acceso a nuestra red cableada.

Se recomienda la instalación de un firewall que filtre el tráfico entre los dos segmentos de red.

2.1.12 Revisar periódicamente la seguridad de la red

Es altamente recomendable analizar de forma periódica el nivel de seguridad de nuestra red. Para ello podemos utilizar las herramientas de wardriving que comentamos en la primera parte de este artículo. Atacar nuestros propia red nos permitirá conocer el nivel de seguridad real en el que nos encontramos.

2.2 Medidas de seguridad detectivas

A pesar de que las medidas de seguridad más importantes (más vale prevenir que curar) se encuentran en el grupo del apartado anterior, no hay que despreciar las medidas de seguridad que comentaremos a continuación y que nos permitirán detectar (más vale tarde que nunca) posibles intrusiones o futuros problemas de seguridad en nuestra red wireless.

2.2.1 Monitorización de la red

Una monitorización de la red nos permitirá identificar intrusiones, mediante el análisis periódico del tráfico:

- Detección de tráfico "sospechoso" (proveniente de estaciones no catalogadas).
- Incremento del ancho de banda ocupado (síntoma de que otras estaciones están utilizando nuestro ancho de banda).

En cuanto a herramientas de monitorización y análisis de redes wireless podemos destacar AirMonitor, desarrollada por OpenWired S.L. y UPCNet. El código de esta herramienta (que requiere Tomcat y Postgres) fue liberado el 3 de junio de 2005 y se encuentra disponible en http://lafarga.upc.es. Esta herramienta permite recopilar datos de la red en tiempo real, localizar los dispositivos existentes, así como visualizar la información de cada dispositivo y usuario inalámbrico conectado.

En la primera parte de este artículo ya se comentaron otras herramientas que nos permitirán monitorizar el tráfico: kismet, airsnort, etherape, etc.

Resulta interesante también revisar periódicamente las ACLs de los APs con el objetivo de identificar alguna MAC que no pertenezca a nuestra red y que pueda haber sido añadida (como puerta trasera, para evitar el filtrado por MAC sin utilizar la MAC del AP) si un intruso se hubiera hecho con el control de nuestro AP.

2.2.2 Habilitar el logging en los dispositivos

Conviene revisar de forma periódica los logs de los distintos dispositivos wireless con el fin de detectar acciones intrusivas o comportamientos anómalos, cosa que nos permitirá corregir deficiencias en las medidas de seguridad adoptadas.

La utilidad de la información facilitada por estos logs es evidente:

- Detección de comportamientos inusuales
- Información para resolver problemas
- Ayuda en procesos de análisis forense
- Evidencia legal

Ya que la tarea de revisión resulta excesivamente tediosa, siempre que sea posible conviene centralizar dichos logs en un único sistema. Como desventajas: existe un único punto de fallo y se requiere redundancia en el almacenamiento.

Syslog es el protocolo utilizado para transportar al servidor central, utilizando el puerto 514 UDP, las comunicaciones de eventos generados por los dispositivos. Syslog se encuentra soportado en UNIX y Linux, en el caso de Windows encontramos soluciones similares. A continuación se enumeran algunas de ellas:

- TriAction Syslog Daemon - http://www.triaction.nl/syslog.htm
- Kiwi - http://www.kiwi-enterprises.com/
- Microtik syslog daemon - http://www.mt.lv/3index.html#utils
- 3COM (free syslog daemon)
  ftp://ftp.3com.com/pub/utilbin/win32/3CSyslog.zip

Como herramientas de análisis de logs, podemos hacer las siguientes referencias:

- logcheck - http://logcheck.org/
- swatch - http://swatch.sourceforge.net/

3 Conclusiones y Recomendaciones

Hemos visto como la aparición del estándar 802.11i ha provocado un aumento más que considerable en la seguridad de las WLAN, ya que proporciona la solución a los problemas clásicos de las redes wireless y que se ponían de manifiesto al utilizar WEP: autenticación, control de acceso y confidencialidad.

También hemos comentado como mejorar la autenticación de usuarios y la integridad y confidencialidad de la información con el uso de VPNs, y como mejorar la calidad del servicio de nuestra red incorporando el estándar 802.11e.

No existe una medida 100% segura, pero nuestro deber es intentar aproximarnos lo máximo posible a ese 100% virtual. Para conseguirlo debemos adoptar el mayor número posible de medidas de seguridad a nuestro alcance.

En cualquier caso, debemos ser conscientes del nivel de seguridad en el que se encuentra nuestra red. A partir de aquí y en función de los servicios ofrecidos y la información que manejamos, tendremos que adoptar las medidas necesarias para alcanzar el nivel de seguridad requerido por nuestras WLAN.

4 Enlaces de Interés

- IEEE
  http://www.ieee.org

- 802.11i
  http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

- Wardrive
  http://www.wardrive.net

5 Glosario

- **802.11e**: Estándar que define un conjunto de capacidades de calidad de servicio para aplicaciones LAN, en particular para el estándar WiFi 802.11. Este estándar está considerado de crítica importancia para aplicaciones como voz sobre IP o streaming multimedia.

- **802.11i**: Estándar que define el cifrado y la autenticación para complementar y mejorar el WEP. Es un estándar que mejorar la seguridad de las comunicaciones mediante el uso del Temporal Key Integrity Protocol (TKIP).

- **AES** (Advanced Encryption Standard): También conocido como Rijndael, es un algoritmo de cifrado de bloque adoptado como un estándar por el gobierno de EEUU, y que fue desarrollado por dos criptógrafos Belgas: Joan Daemen y Vincent Rijmen.

- **DoS** (Denial of Service): Tipo de ataque cuyo objetivo es inutilizar un sistema, servicio o red, de forma que deje de prestar el servicio que ofrecía. Muchos de estos ataques (Ping of Death, Teardrop, ...) explotan limitaciones de los protocolos TCP/IP.

- **IEEE** (Institute of Electrical and Electronics Engineers): Organización compuesta por ingenieros, científicos y estudiantes, conocida por desarrollar estándares para la industria informática y electrónica. En particular, los estándares IEEE 802 para redes de área local son ampliamente seguidos.

- **QoS** (Quality of Service): Conjunto de tecnologías que permiten a las aplicaciones de red, solicitar y recibir niveles de servicio en ancho de banda, propagación y variaciones de retardo (jitter).

- **Wi-Fi** (Wireless Fidelity): Término usado de forma genérica para referirse a cualquier tipo de red 802.11. El término fue acuñado por la Wi-Fi Alliance.

- **WPA2** (Wi-Fi Protected Access 2): Es la segunda generación de WPA. Provee a los usuarios Wi-Fi de un alto nivel de seguridad, asegurando que sólo usuarios autorizados pueden acceder a sus redes wireless.