MEMORIA DEL PROYECTO FINAL DE CARRERA

Título: Seguridad en redes sin hilos: Wifi y Wimax

Autor: Antonio Delgado Martínez

Contacto: adelgadomart@uoc.edu

Titulación: Ingeniería Técnica de Telecomunicaciones, especialidad en Telemática

Director del proyecto: José López Vicario

<u>Agradecimientos</u>

A mi pareja Verónica por todo su apoyo y cariño.

A mi padre y abuelo Félix por toda la ayuda ofrecida.

Y a mis padres, José y Toñi, a los cuales dedico en especial este proyecto y que siempre echare de menos.

Índice general

1. Introducción

1.1 Justificación y motivos del proyecto

El motivo por el que se quiso iniciar este proyecto sobre el estudio de las redes de infrarrojos, bluetooth, 3G, Wifi y Wimax, fue por el gran papel que juegan estas en la sociedad actual. A través del uso malicioso de cada una de estas redes, un hacker o un atacante puede dañar en gran manera no solo al dispositivo atacado, sino al propio usuario que hace uso de él. Evidentemente no nos estaremos refiriendo a un daño físico, sino a un daño de robo de identidad, de dinero, de información personal u otros.

Es por esto básicamente por lo que se decidió en realizar este proyecto, ya que además de resultar muy interesante se hace muy útil el poder estudiar los diferentes ataques, así como las soluciones y las medidas de seguridad implementadas en cada una de las 5 redes elegidas.

1.2 Objetivos del proyecto

La intención o finalidad de este proyecto ha sido la de realizar un estudio completo de las 5 redes de las que consta el proyecto, haciendo especial énfasis a las redes Wifi y Wimax. Asimismo también se ha querido demostrar y explicar cómo defenderse de estos ataques y que pautas o medidas son recomendables para evitar todos estos. Es decir, este proyecto se podría definir como una guía o manual en el que se muestran los ataques y problemas más comunes para cada una de las redes, donde además se darán una serie de soluciones, consejos y recomendaciones, aunque por supuesto habiendo estudiado con anterioridad que son y cómo se comportan cada una de estas redes.

Lo que se persigue principalmente con la lectura de este proyecto es que todo aquel usuario que lo lea haya adquirido conocimientos sobre:

- Que son, cuales son las ventajas y desventajas, y como trabajan las 5 redes estudiadas, en especial Wifi y Wimax.
- Cuál es la seguridad implementada por cada red y que mecanismos utilizan cada una de estas.
- Que ataques son más comunes en cada una de las redes y que medidas hay que llevar a cabo para evitar estos.
- Que problemas pueden ofrecer generalmente los dispositivos hardware de las diferentes redes y cuáles pueden ser las posibles causas y soluciones.
- Como configurar manualmente dispositivos para lograr una óptima seguridad.
- Cuáles son las diferencias entre Wifi y Wimax.
- Que programas de software son recomendables para garantizar la seguridad de los equipos.

1.3 Equipo y tecnología empleada

Para el desarrollo de todo este proyecto se han utilizado los siguientes equipos:

- Ordenador portátil Asus N55S, teniendo como prestaciones:
  - Procesador Intel Core i7-2670QM CPU @ 2.20GHz.
  - 750 GB de memoria.
  - 8 GB de memoria RAM.
  - Sistema operativo: Windows 7 Home Premium.
- Teléfono móvil Samsung Galaxy SII.
- Router JAZZTEL AR-5387.

Por otro lado, el software que se ha utilizado para desarrollar el proyecto ha sido:

- Entorno de máquinas virtuales ORACLE VM Virtual Box.
- Sistema operativo Linux, versión Ubuntu (corriendo en máquina virtual).
- Sistema operativo Windows 7 (corriendo en Asus N55S).
- Software de intrusion: Wifiway, Wifislax 4.3, Aircrack.
- Software de prevención: ADSL Net, NETCUT.
- Microsoft Word, Microsoft PowerPoint y GanttProject.

1.4 Planificación del proyecto

La forma de ejecución de este proyecto se ha desarrollado de una manera progresiva, donde se han ido realizando los diferentes puntos del proyecto uno por uno. La manera en la que se ha ido avanzado en el proyecto bien se puede dividir en 5 partes principales, haciendo estas 5 partes referencia a las diferentes PECs que se han realizado a lo largo de la asignatura.

Explicaremos a continuación que se hizo en cada una de estas 5 partes o PECs:

- PEC 1

Esta primera se podría definir como la parte de definición e introducción del proyecto. En esta pec se llevó a cabo lo siguiente:

- Elección de los diferentes objetivos y temas a tratar en el proyecto.
- Elección de un formato adecuado para el proyecto.
- Primera búsqueda de información.
- Creación de la planificación a seguir durante el resto del proyecto.
- Puesta a punto, comprobación y descarga de los diferentes equipos o software a utilizar en el transcurso del proyecto.

- PEC 2

La PEC 2 corresponde con la parte más teórica del proyecto en sí, siendo el principal objetivo de esta establecer las bases teóricas de las diferentes redes con el fin de tener claros los conceptos de cada una de estas. Concretamente en esta PEC se desarrollaron los siguientes puntos:

- Comparación general entre Wifi y Wimax.
- Definición y estudio de las 5 redes elegidas.
- Definición de las ventajas/desventajas de las 5 redes.
- Estudio sobre los posibles usos, problemas, causas y soluciones de todas las redes.
- Estudio de la seguridad implementada en cada una de las redes.
- Primera estudio sobre los diferentes ataques y recomendaciones de seguridad de infrarrojos, bluetooth y 3G.
- Nueva búsqueda de información y primer esbozo de bibliografía y glosario.

- PEC 3

La ultima PEC o PEC 3 corresponde en este caso con la parte más práctica y técnica del proyecto, haciendo de ella sin duda alguna la más importante del proyecto. Es esta PEC donde por fin el proyecto se completa en su totalidad. Para conseguir esto se llevaron a cabo los siguientes puntos:

- Modificación de varios apartados anteriores atendiendo a los consejos ofrecidos por el tutor.
- Creación de simulaciones para todas las redes a excepción de la red de infrarrojos.
- Inclusión de nuevos ataques, recomendaciones, problemas y usos a los ya definidos en la PEC 2.
- Estudio de los diferentes ataques, vulnerabilidades, recomendaciones y programas de software para las redes de Wifi y Wimax.
- Inclusión de anexos y finalización de la bibliografía y el glosario.
- Revisión final y entrega del proyecto.

- Memoria y Presentación

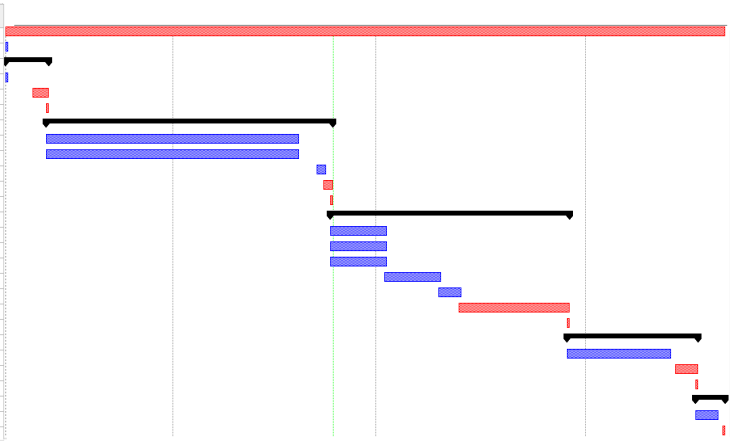
Esta parte corresponde a la parte final de la asignatura donde se han llevado a cabo los siguientes puntos:

- Se ha realizado la memoria final de proyecto, siendo esta un entregable de síntesis donde se han reflejado las partes más importantes y destacables que se han podido estudiar a lo largo de proyecto.
- Se ha realizado la presentación virtual, la cual recoge los puntos más generales e importantes del proyecto.

- Diagrama de Gantt

Para finalizar este apartado exponemos a continuación la consiguiente planificación mediante un diagrama de Gantt, quedando reflejado en este todas las tareas realizadas y el tiempo que se ha dedicado para una de estas.

Nombre	Duracion	Inicio	Terminado
TFC-Seguridad en redes sin hilos	77 days	7/03/13 8:00	21/06/13 17:00
Inicio TFC	1 day	7/03/13 8:00	7/03/13 17:00
PEC 1	5 days	**7/03/13 8:00**	**13/03/13 17:00**
Descripción y objetivos	1 day	7/03/13 8:00	7/03/13 17:00
Planificación	3 days	11/03/13 8:00	13/03/13 17:00
Entrega PEC 1	1 day	13/03/13 8:00	13/03/13 17:00
PEC 2	31 days	**13/03/13 8:00**	**24/04/13 17:00**
Busqueda de información y contenidos	28 days	13/03/13 8:00	19/04/13 17:00
Realizacion apartados 2, 3, 4, 5, 6	28 days	13/03/13 8:00	19/04/13 17:00
Realización apartado 1	2 days	20/04/13 8:00	23/04/13 17:00
Repaso final antes de entregar	2 days	23/04/13 8:00	24/04/13 17:00
Entrega primera parte del proyecto	1 day	24/04/13 8:00	24/04/13 17:00
PEC 3	26 days	**24/04/13 8:00**	**29/05/13 17:00**
Busqueda de informacion y contenidos	7 days	24/04/13 8:00	2/05/13 17:00
Realizacion apartado 9	7 days	24/04/13 8:00	2/05/13 17:00
Realizacion apartado 7	7 days	24/04/13 8:00	2/05/13 17:00
Realizacion apartado 8	7 days	2/05/13 8:00	10/05/13 17:00
Repaso global proyecto	2 days	10/05/13 8:00	13/05/13 17:00
Empezar a realizar la memoria	13 days	13/05/13 8:00	29/05/13 17:00
Entrega segunda parte del proyecto	1 day	29/05/13 8:00	29/05/13 17:00
Memoria final	14 days	**29/05/13 8:00**	**17/06/13 17:00**
Terminar memoria final	12 days	29/05/13 8:00	13/06/13 17:00
Revisión final de la memoria	2 days	14/06/13 8:00	17/06/13 17:00
Entrega memoria final del proyecto	1 day	16/06/13 8:00	17/06/13 17:00
Presentación	5 days	**17/06/13 8:00**	**21/06/13 17:00**
Elaborar presentación	4 days	17/06/13 8:00	20/06/13 17:00
Entrega presentación	1 day	21/06/13 8:00	21/06/13 17:00



2. Descripción tecnologías existentes y relacionadas con el proyecto

Como bien hemos dicho en el primer punto de esta memoria, el proyecto se ha desarrollado sobre 5 tipos de redes sin hilos, las cuales son: infrarrojos, Bluetooth, 3G, Wifi y Wimax.

Estudiaremos a continuación de una manera breve cada una de estas redes:

2.1 Infrarrojos

Este tipo de red utiliza la radiación infrarroja para comunicar diferentes nodos o dispositivos, utilizando para esto una serie de leds infrarrojos instalados tanto en el emisor como en el receptor. El funcionamiento de los dispositivos de las redes de infrarrojos se basa principalmente en la modulación y desmodulacion por parte del emisor y del receptor respectivamente.

2.2 Bluetooth

El bluetooth es una tecnología exclusivamente inalámbrica la cual trabaja con ondas de radio de corto alcance que a diferencia de los infrarrojos, sí que pueden atravesar obstáculos. Su espectro de frecuencia está comprendido entre 2.4 y 2.485GHz, donde además trabajará sobre una banda libre. Su principal función es la de comunicar varios dispositivos en un radio de corto alcance a través de radiofrecuencia.

2.3 Tercera generación/3G

La 3G o tercera generación de telefonía móvil corresponde a la generación actual de telefonía, la cual gracias a las diversas tecnologías y estándares implementados en esta ofrece una gran variedad de servicios y posibilidades. Entre todos los servicios que esta tercera generación ofrece los más importantes y utilizados son los siguientes: acceso a internet, interoperabilidad, servicios de banda, videollamadas, roaming internacional, uso simultaneo tanto de voz como de datos, descarga de programas, correos electrónicos y mensajería instantánea.

Todos estos servicios son posibles gracias a las diversas tecnologías y estándares que constituyen el 3G, como por ejemplo la UMTS, cuyas características principales son: capacidades multimedia, velocidad de acceso a internet elevada y una transmisión de voz con una calidad equiparable a la de las redes fijas.

2.4 Wifi

La tecnología Wifi es la tecnología por excelencia de todos los hogares con conexión a internet. Su método de funcionamiento está basado en la utilización de ondas de radio, puede ofrecer diferentes velocidades de conexión y es utilizada normalmente para entornos de oficinas y domésticos. Wifi es una marca de la Wi-fi Alliance, que es la organización o compañía que certifica y prueba que los equipos cumplen los estándares 802.11.

Se pueden encontrar multitud de diferentes estándares Wifi, donde según el elegido este nos ofrecerá un conjunto de posibilidades y características diferentes respecto a los demás.

2.5 Wimax

La tecnología Wimax es una tecnología basada en IP, de acceso inalámbrico digital de banda ancha que ofrece unas prestaciones y un rendimiento similar a las redes 802.11, pero con la cobertura y la calidad de servicio (QoS) de las redes telefónicas.

El estándar sobre el que se basa toda la tecnología Wimax es el 802.16. Este estándar destina su uso hacia redes de área metropolitana o redes WMAN, proporcionando acceso inalámbrico de hasta aproximadamente 60km para estaciones fijas, y hasta 15km para estaciones móviles. Se diferencian varias frecuencias de trabajo, más concretamente de 2.3 a 3.5GHz y de 5.4GHZ.

El único organismo regulador que está habilitado para certificar el cumplimiento de las prestaciones y características ofrecidas por el estándar, así como la interoperabilidad entre equipos de diferentes marcas es el Wimax Fórum. Por consiguiente todo equipo que no cuente con la debida certificación no puede garantizar la interoperabilidad entre diferentes productos.

3 Resultados obtenidos

Ya terminada la parte teórica pasaremos ahora a ver de una forma resumida los diferentes resultados que se han obtenido para cada una de las redes. Más concretamente en este apartado se verá para cada red:

- Usos: en este apartado se ha querido ofrecer una serie de usos y aplicaciones para cada tipo de tecnología, con el fin de que quede reflejado para que se puede emplear cada tipo de red y con qué fines.
- Problemas, causas y soluciones: este apartado hace referencia a una serie de problemas que se podrán encontrar al hacer uso de cada una de estas tecnologías, tanto a nivel de hardware como de software. Asimismo también se reflejan las posibles causas de cada problemas y las posibles soluciones.
- Seguridad: en el apartado de seguridad se ha querido reflejar la seguridad implementada en cada una de las redes estudiadas, puesto que esta se hace indispensable a la hora de intentar evadir los posibles ataques.
- Ataques y recomendaciones: la intención de este apartado ha sido el enumerar y explicar los ataques más importantes que cada una de las 5 redes suelen recibir, donde además se han listado una serie de recomendaciones y consejos para intentar evadir y minimizar el riesgo de recibir cualquiera de estos ataques.
- Software de intrusión y de protección para Wifi y Wimax: en este apartado se han enumerado varios programas de software (los cuales se encuentran descritos en el proyecto técnico), donde cada uno de estos estará orientado a un determinado uso.
- Simulaciones: para este último apartado se han llevado a cabo de forma práctica varias de las recomendaciones mencionadas en el apartado de ataques, con el fin de que se pueda estudiar el cómo configurar ciertos dispositivos de forma segura respecto a las características y posibilidades del dispositivo o equipo.

3.1 Usos

Reflejaremos a continuación los diferentes usos de cada una de las tecnologías estudiadas:

3.1.1 Infrarrojos

La tecnología infrarroja permite la comunicación a través de la transferencia de información entre diferentes nodos o dispositivos que estén conectados entre sí. Uno de los ejemplos más comunes respecto a redes de infrarrojos es la comunicación entre un ordenador y una impresora o algún tipo de periférico, pero como se va a ver a continuación existen muchas más posibilidades de conexión.

Los posibles usos son:

- Conexión entre ordenador y periféricos.
- Conexión entre ordenadores.
- Conexión de diferentes dispositivos.
- Conexión entre móviles.
- Conexión entre edificios o puntos muy lejanos.

3.1.2 Bluetooth

La tecnología Bluetooth está orientada a la comunicación de diferentes dispositivos en un radio de corto de alcance. Las aplicaciones y usos para los que está destinado el Bluetooth son los siguientes:

- Comunicación entre dispositivos móviles.
- Comunicación o enlaces entre distintos dispositivos que implementen Bluetooth.
- Creación de redes inalámbricas.
- Transferencia de archivos, voz y datos.
- Visión remota.
- Sincronización automática.
- Manos libres.
- Utilizar el teléfono móvil como control remoto.

3.1.3 Tercera generación/3G

Al igual que las dos anteriores tecnologías ya descritas, el 3G también ofrece un amplio repertorio de posibles usos y aplicaciones:

- Transmisión de voz y datos y video.
- Transmisión de datos no-voz.
- Alta velocidad de acceso a internet y banda ancha.
- Roaming internacional.
- Interoperabilidad.
- Otros servicios.

3.1.4 Wifi

Esta tecnología posee un amplio abanico de usos, por lo que enunciaremos los más comunes y útiles de esta tecnología:

- Uso personal.
- Redes LAN en escenario doméstico o empresarial.
- Servicios de redes privadas.
- Usos industriales
- Motivos arquitectónicos.
- Hot Spot.
- Convertir a un Smartphone en control remoto.
- Ofrecer internet a otros dispositivos que no sean ordenadores.
- Intercambio de información entre diferentes dispositivos.
- Convertir nuestro móvil en un punto de acceso a internet Wifi.
- Ver películas en línea desde cualquier televisor de nuestra casa.

3.1.5 Wimax

Los usos definidos para la tecnología Wimax son los siguientes:

- Interconexión de varios nodos.
- Acceso a internet.
- Comunicaciones Wimax-Wifi.
- Proporcionar internet en zonas determinadas.
- Comunicación y transferencia de gran cantidad de servicios.
- Rápida infraestructura en desastres naturales o situaciones críticas.
- Ámbito doméstico.

3.2 Problemas, causas y soluciones

A continuación se van a exponer varios problemas con sus posibles causas y soluciones.

3.2.1 Infrarrojos

Varios problemas que podremos encontrar en los dispositivos infrarrojos son los siguientes:

Problema	Causa	Solución
La señal ha sido enviada pero no ha llegado al receptor.	-La alineación entre ambos nodos no es la correcta. -La señal se ha encontrado con demasiadas interferencias u obstáculos llegando a desaparecer por completo.	-Comprobar la alineación y corregirla en caso necesario. -Intentar encontrar otro método o camino por el que enviar la información.

	-La señal ha desaparecido al instante debido a un obstáculo.	-Eliminar obstáculo en caso de que se pueda. En caso contrario encontrar otro camino o método para enviar la información.
	-La señal ha sido atenuada pero no ha desaparecido.	-Aumentar la sensibilidad del receptor o encontrar otra forma o método de enviar la señal.
	-En caso de transmitir en modo cuasi-difuso, la alienación de los diferentes componentes no es correcta.	-Comprobar la alineación y corregirla en caso necesario.
	-La frecuencia del reloj esta descompensada.	-Calibrar la frecuencia. Normalmente para la comunicación entre diferentes dispositivos la frecuencia idónea de cada dispositivo dependerá del propio dispositivo en concreto.
	-En caso de pequeñas comunicaciones entre dispositivos se puede haber sobrepasado la distancia efectiva.	-Acerca el dispositivo emisor al receptor.
La señal no puede enviarse.	-Fuente de alimentación agotada.	-Recargar o sustituir la fuente de alimentación.
	-Diodo emisor averiado.	-Reparar o sustituir el diodo averiado.
	-Avería de otro componente del dispositivo emisor.	-Sustituir o reparar el dispositivo emisor o el componente dañado.
	-No hay potencia suficiente.	-Incrementar la potencia.
La señal ha llegado físicamente al receptor pero este no puede trabajar con ella.	-Diodo receptor averiado.	-Reparar o sustituir el diodo receptor.
	-Avería de otro componente del dispositivo receptor.	-Sustituir o reparar el dispositivo receptor o el componente dañado.

	-La codificación utilizada en ambos dispositivos no es la misma.	-Cambiar la codificación utilizada.
	-El dispositivo receptor no posee o no tienen bien configurado el puerto de infrarrojos.	-Verificar y en caso necesario configurar adecuadamente este.
	-No se han listado correctamente los drivers.	-Algunos dispositivos necesitan configurar adecuadamente los drivers antes de iniciar la conexión, por lo que es conveniente revisar estos.
	-El puerto receptor no está activado.	-Activar el puerto.
La transferencia de datos es lenta o errónea.	-El hardware no funciona correctamente.	-Comprobar las soluciones anteriores.
	-Hay obstáculos o interferencias entre los dispositivos.	-Eliminar dichas interferencias y obstáculos.
	-Se ha instalado de manera errónea un controlador.	-Actualizar los controladores más recientes que se encuentren disponibles, así como asegurarse de quitar los viejos antes de instalar nuevos.
	-El método de transferencia de datos no es compatible entre dispositivos.	-Verificar que ambos métodos coincidan.
	-El adaptador de infrarrojos está conectado a un dispositivo más lento.	-Adaptar y limitar la velocidad respecto a las prestaciones del dispositivo más lento. Normalmente esta velocidad suele ser de 19,2Kbps.
	-Si se utiliza un puerto serie (COM), el controlador del puerto de serie ha restaurado de forma errónea la configuración.	-Seguir estos pasos: Inicio -> Ejecutar (escribimos regedit) y aceptamos. Desde el menú Edición damos a nuevo y a continuación a Valor DWORD.

		Escribimos "SerialRelinquishPowerPolicy" y aceptamos. Desde el menú Edición damos a modificar y en el cuadro de información de valor escribimos 1. Aceptamos y salimos.
La señal ha sido interceptada.	-La señal ha sido interceptada por receptor no deseado.	-En interiores, aislar adecuadamente las posibles zonas por las que se pueda escapar la señal. -En caso de exteriores, buscar un camino o método diferentes por el que transmitir la información.
No hay puerto de infrarrojos para conexión directa por cable o el puerto no se puede abrir.	-No se han configurado correctamente los puertos a utilizar. -Si se muestra un error de software, es probable que el software este desactualizado -No se ha seleccionado el puerto correcto.	-Configurar correctamente los puertos y asegurarse de la compatibilidad de ambos. -Buscar y actualizar a la versión más reciente. -Verificar y en caso necesario seleccionar el puerto correcto.
No se puede instalar un dispositivo infrarrojo en un PC.	-Los drivers han sido mal instalados o falta alguno de estos. -Se está intentando instalar por un puerto incorrecto. -El dispositivo no ha podido instalarse o no ha sido reconocido. -No se ha configurado previamente la BIOS. -El equipo no dispone de puerto infrarrojo.	-Verificar y en caso necesario reinstalar o instalar nuevos drivers. -Consultar el manual de la placa y averiguar el puerto correcto. -Expulsar y reintentar nuevamente la conexión. -Consultar el manual del equipo, concretamente la configuración de nuevos dispositivos infrarrojos. -No se puede determinar solución alguna a esta causa.

	-Si se muestra un error "Administrador de dispositivo", hay un problema con el controlador de la interfaz LPC.	-Seguir los siguientes pasos: desactivar el infrarrojo, entrar a configuración de BIOS -> configuración de dispositivos periféricos, deshabilitar Enhaced Consumer IR, guardar y salir.

3.2.2 Bluetooth

Al igual que con infrarrojos, en Bluetooth también se pueden encontrar multitud de problemas:

Problema	Causa	Solución
Se reciben mensajes o archivos no deseados (Bluejackiing).	-El Bluetooth está en modo visible y sin ningún tipo de seguridad.	-Ponerlo en modo no visible o habilitar clave de paso.
No podemos conectarnos a una red creada.	-Limitación de dispositivos conectados alcanzada. -Bluetooth en modo no visible.	-Esperar a que un dispositivo abandone dicha red. -Poner el Bluetooth en modo visible.
Nuestro dispositivo no reconoce un dispositivo habilitado con Bluetooth antes de agregarlo.	-El otro dispositivo no se ha inicializado correctamente. -El otro dispositivo no dispone de batería o está apagado. -El otro dispositivo tiene el Bluetooth en modo no visible. -El alcance entre dispositivos es superior al alcance efectivo. -Dispositivo dañado. -Se necesita configurar un puerto COM.	-Quitar el dispositivo y reiniciarlo debidamente. -Conectar el dispositivo a una fuente de alimentación y encenderlo. -Activar debidamente el Bluetooth. -Reducir la distancia entre dispositivos. -Reparar o cambiar el dispositivo dañado. -Configurar un puerto COM conforme a lo requerido.
Una vez agregado el dispositivo, este no se reconoce.	-Falta de alimentación del dispositivo. -Fallo de software.	-Conectarlo a una fuente de alimentación y reintentar. -Actualizar el dispositivo a la

		versión más reciente.
	-Fallo temporal de reconocimiento.	-Reintentar nuevamente la conexión.
Dos dispositivos no pueden comunicarse. En este caso no habrá problemas de reconocimiento.	-Uno de los dos dispositivos está ocupado o tiene demasiadas conexiones.	-Esperar y reintentar cada cierto tiempo.
	-Se ha establecido conexión con un dispositivo no deseado.	-Verificar y conectar con el dispositivo deseado.
	-Clave de paso mal escrita.	-Introducir nuevamente la clave de paso.
	-Imposibilidad de conectar debido a interferencias muy fuertes. Entran en este grupo: microondas, redes inalámbricas 802.11, teléfonos inalámbricos y controles remotos de equipos electrónicos.	-Alejarse de la posible fuente de interferencia y volver a intentar.
La conexión con otro dispositivo es lenta, intermitente o defectuosa.	-El alcance entre dispositivos es superior al alcance efectivo.	-Reducir la distancia entre dispositivos.
	-Exceso de dispositivos vinculados o conexiones.	-Esperar a que el dispositivo este menos ocupado.
	-Imposibilidad de conectar debido a interferencias muy fuertes. Entran en este grupo: microondas, redes inalámbricas 802.11, teléfonos inalámbricos y controles remotos de equipos electrónicos.	-Alejarse de una posible fuente de interferencias y volver a intentar.
	-Se ha restablecido la seguridad en uno de los dispositivos.	-Reiniciar o reinstalar el sistema operativo del dispositivo en concreto.
	-Problema interno del propio dispositivo (varios modelos de Nokia han registrado este tipo de fallo).	-Descargar última versión de firmware.

Se ha olvidado la clave de paso.	-En caso de tener habilitada la clave de acceso será obligatorio introducirla.	-En sistemas Windows la clave por defecto suele ser 0000 o 0001. En caso de que haya sido modificado y olvidada ponerse en contacto con el servicio técnico.
El dispositivo ha sido infectado.	-Se ha introducido un virus en el sistema (esto solo suele pasar en los sistemas Symbian OS serie 60).	-Eliminar virus, formatea dispositivo o consultar servicio al servicio técnico (lo referente a seguridad y ataques se ver más adelante).

3.2.3 Tercera generación/3G

Varios problemas que se pueden encontrar en la tecnología 3G son los siguientes:

Problema	Causas	Solución
No se pueden realizar o recibir llamadas.	-Modo avión activado.	-Desactivar el modo avión.
	-No hay cobertura.	-Cambiar de ubicación o salir al exterior.
	-Fallo en los ajustes de red.	-Restablecer los ajustes de red desde el propio dispositivo.
	-Fallo en la tarjeta SIM.	-Sacar la tarjeta SIM, limpiarla, comprobar que no está dañada e introducirla cuidadosamente de nuevo en el dispositivo.
	-Avería o rotura en la tarjeta SIM.	-Cambiar tarjeta SIM.
	-Dispositivo no actualizado.	-Actualizar el dispositivo.
	-Rotura de algún componente sensible relacionado con la conexión del dispositivo.	-Reparar el componente o cambiar de dispositivo.
	-3G no configurado.	-Configurar correctamente el 3G.

	--Caída temporal de la red.	-Esperar a que la red vuelva nuevamente.
	-Otros problemas.	-Contactar con servicio técnico.
La conexión y transferencia de archivos por Internet es lenta o intermitente.	-Modo avión activado.	-Desactivar el modo avión.
	-El dispositivo está en movimiento.	-Disminuir la velocidad de movimiento o detenerlo.
	-No hay cobertura.	-Cambiar de ubicación, salir al exterior o intentar conectarse a otra red (Wifi).
	-En caso de estar conectados a una red Wifi, la señal es muy débil.	-Acercarse al dispositivo emisor.
	-En caso de estar conectados a una red Wifi, la conexión sigue siendo lenta o intermitente.	-Deshabilitar la conexión Wifi y conectarse a la red 3G.
	-Fallo en los ajustes de red.	-Restablecer los ajustes de red desde el propio dispositivo.
	-Fallo en la tarjeta SIM.	-Sacar la tarjeta SIM, limpiarla, comprobar que no está dañada e introducirla cuidadosamente de nuevo en el dispositivo.
	-Avería o rotura en la tarjeta SIM.	-Cambiar tarjeta SIM.
	-Dispositivo no actualizado.	-Actualizar el dispositivo.
	-Rotura de algún componente sensible relacionado con la conexión del dispositivo.	-Reparar el componente o cambiar de dispositivo.
	-3G no configurado.	-Configurar correctamente el 3G.
	-Caída temporal de la red.	-Esperar a que la red vuelva

		nuevamente.
	-Otros problemas.	-Contactar servicio técnico.
El dispositivo no se puede conectar a una red Wifi.	-La opción Wifi del dispositivo esta desactivada.	-Activar la señal Wifi.
	-El dispositivo emisor de la señal Wifi está desactivado.	-Activar el correspondiente dispositivo.
	-La red Wifi a la que se ha intentado conectar no es la deseada.	-Comprobar el listado de conexiones y en caso erróneo conectarse a la red deseada.
	-La señal recibida es muy débil.	-Acercarse al dispositivo emisor.
	-Red protegida.	-Introducir contraseña, en caso de conocer la contraseña contactar con el administrador de la red Wifi.
	-Contraseña incorrecta.	-Quitar la omisión de caracteres y verificar que se está introduciendo debidamente la contraseña. En caso de olvido contactar con el administrador de la red Wifi.
-El dispositivo está conectado a Wifi, pero no se puede acceder a internet.	-Señal débil.	-Acercarse al dispositivo emisor.
	-Los paquetes están deshabilitados.	-Activar los paquetes de datos desde el correspondiente menú.
	-Error o modificación en datos de puntos de acceso.	-Verificar y editar los datos en caso erróneo.

3.2.4 Wifi

Los posibles problemas de Wifi son los siguientes:

Problema	Causa	Solución
Velocidad lenta o intermitente.	-Exceso de personas conectadas a un mismo punto de acceso.	-Esperar a que el punto de acceso este menos ocupado, utilizar otro punto de acceso o incrementar la velocidad del punto de acceso actual.
	-Interferencias o pérdidas entre el punto de acceso y el receptor.	-Aproximarse al dispositivo emisor, aumentar la señal, cambiar el canal o intentar eliminar las posibles fuentes de interferencias o pérdidas.
	-Problema temporal en la línea.	-Esperar a que la línea vuelva a la normalidad.
	-Daño en el dispositivo emisor o receptor.	-Reparar o sustituir el dispositivo dañado.
	-Se ha superado la distancia efectiva del dispositivo emisor.	-Acercarse al dispositivo emisor.
El dispositivo emisor no emite señal Wifi.	-Problema temporal en la línea.	-Esperar a que la línea vuelva a la normalidad.
	-El dispositivo no está configurado correctamente.	-Configurar correctamente los ajustes Wifi del router.
	-Fallo en instalación.	-Comprobar los cables conectados al router.
	-Fallo temporal en el dispositivo emisor.	-Reiniciar el dispositivo.
El dispositivo receptor no recibe la señal o no encuentra la red.	-Se ha conectado o se está intentando conectar a un dispositivo emisor diferente.	-Comprobar el listado de redes disponibles y verificar a cual se ha conectado o se está intentando conectar.
	-El dispositivo emisor no emite señal Wifi.	-Consultar las posibles causas en el apartado anterior.
	-La señal llega demasiado debilitada o se ha perdido a lo largo del medio.	-Aproximarse hacia el dispositivo receptor, cambiar el canal, aumentar la señal o intentar eliminar posibles

		fuentes de interferencias o pérdidas.
	-Problema temporal en el router.	-Reiniciar el router.
	-Red no visible.	-Por cuestiones de seguridad algunas redes no muestras su SSID, por lo que se tendrá que cambiar la configuración del router para poder encontrar la red.
	-Se ha superado el rango de alcance del dispositivo emisor.	-Acercarse al dispositivo emisor.
	-Ajustes de red mal configurados.	-Comprobar los ajustes de red y en caso necesario modificar estos.
-La clave no funciona.	-Se ha introducido una clave incorrecta.	-Omitir la omisión de caracteres y asegurarse de que escribimos correctamente la clave.
	-La clave se ha olvidado.	-Resetear el router y configurar nuevamente este.
-El icono de redes aparece pero no funciona.	-Se ha producido largo de inactividad y el PC ha desactivado la opción Wifi para ahorra energía.	-Conectar nuevamente el Wifi.
	-La opción Wifi esta desactivada.	-Activar nuevamente esta opción.
	-Problema temporal en el router.	-Reiniciar el router.
	-Fallo o daño en el adaptador de red.	-Verificar el adaptador de red utilizado. En caso de daño sustituir este.
-La red ha sido infectada o hackeada.	-Se ha introducido software malicioso o un hacker está siendo atacado por un hacker.	-Todo lo relacionado con seguridad se puede encontrar en el apartado de seguridad.

-La conexión se desconecta y se reconecta con regularidad.	-Interferencia con otras redes Wifi.	-Cambiar el canal que se utilizando actualmente. Si el problema persiste cambiar nuevamente el canal.
	- Problema de hibernación de la tarjeta Wifi.	-Desmarcar la opción "autorizar al sistema a apagar este periférico" desde las opciones Wifi.
	-Interferencias con hornos microondas, Bluetooth, ZigBee o teléfonos inalámbricos.	-Alejar o desconectar las posibles fuentes de interferencia.
	-Protocolo inestable. Ciertos protocolos de red (por ejemplo Aegis) son inestables.	-Desinstalar protocolo.
	-La frecuencia de difusión no es óptima. Algunas marcas pueden tener ciertas preferencias respecto al canal de transmisión.	-Cambiar el canal de transmisión utilizado. Las marcas Dlink, Netgear, Linksys, entre otras funcionan mejor en canales elevados como el 10 o el 11.
-Estando conectado a una red Wifi no se puede acceder a Internet.	-Se ha conectado a una red errónea o no deseada.	-Comprobar a que red se está conectado y en caso necesario conectar a la deseada.
	-Los ajustes Wifi no son correctos.	-Configurarlos correctamente.
	-No se tiene permiso para acceder a Internet.	-Cambiar de punto de acceso o solicitar permiso.
	-La red Wifi utiliza filtrado de direcciones MAC.	-Añadir su dirección MAC a la lista de acceso del router Wifi.

3.2.5 Wimax

Por ultimo en el apartado de problemas tendremos los correspondientes a la tecnología Wimax:

Problema	Causa	Solución
-La señal Wimax ha sido emitida pero no se puede conectar a la red.	-Se encuentra fuera del rango de alcance efectivo.	-Situarse dentro del radio efectivo.
	-No se dispone de un dispositivo PCMCIA o USB instalado en el dispositivo.	-Instalar y configurar correctamente el dispositivo a utilizar.
	-El interruptor físico de la señal de radio está apagado.	-Verificar y en caso necesario encender este.
	-La señal ha sido debilitada debido a posibles interferencias (otros accesos inalámbricos u hornos microondas).	-Alejarse de los posibles puntos de interferencias.
	-La señal Wifi y Wimax están encendidos simultáneamente (no pueden trabajar a la vez).	-Apagar la señal Wifi y conectar únicamente la señal Wimax.
	-Caída temporal de la línea.	-Esperar a que la línea vuelva a la normalidad.
	-Fallo en el software de Wimax.	-Restaurar y reparar el correspondiente software.
	-El interruptor inalámbrico está apagado.	-Encender el correspondiente interruptor.
	-El controlador Wimax esta desactualizado.	-Comprobar las últimas actualizaciones y en caso necesario instalar la más reciente.
	-La cuenta del usuario esta desactivada.	-Activar la cuenta de usuario.
-La conexión es muy lenta o se pierde a intervalos.	-Se encuentra fuera del rango de alcance efectivo.	-Situarse dentro del radio efectivo.
	-La señal ha sido debilitado debido a posibles interferencias (otros accesos inalámbricos u hornos microondas).	-Alejarse de los posibles puntos de interferencias.

-La red ha sido infectada o hackeada.	-Se ha introducido software malicioso o un hacker está siendo atacado por un hacker.	-Todo lo relacionado con seguridad se puede encontrar en el apartado de seguridad.
-Estando conectado a una red el servicio de internet no funciona.	-Restricción de acceso en el dispositivo receptor. -Problema temporal de la línea.	-Configurar adecuadamente los puertos y eliminar posibles restricciones. -Esperar que la línea vuelva a la normalidad.

3.3 Seguridad

Se analizara ahora de una forma breve la seguridad implantada en cada una de las tecnologías estudiadas.

3.3.1 Infrarrojos

La seguridad en las comunicaciones por infrarrojos se puede decir que es la más simple de todas en comparación con otras redes de tipo inalámbrico. La seguridad de estas redes gira en torno al estándar utilizado y al direccionamiento de la señal infrarroja.

1. Direccionamiento

Una de las ventajas que ofrecen los infrarrojos a la hora de la seguridad es que la señal infrarroja no puede atravesar obstáculos. Por tanto en esta parte la seguridad depende únicamente del usuario, el cual debe asegurarse de que la señal no pueda escapar y poder llegar a receptor no deseados.

2. Estándares

2.1 REC80

Usa modulación de ancho de pulso. Cada bit transmitido es codificado por un nivel alto de duración T seguido de un nivel bajo de duración 2T en caso de que se codifique un cero lógico, o de un nivel alto de duración 3T en caso de que se codifique un uno lógico. Cabe decir que este estándar está prácticamente en desuso.

2.2 RC5

En este caso los 0 lógicos se codifican mediante un flanco negativo (transición alto bajo) mientras que los 1 lógicos mediante un flanco positivo (transición bajo alto). Este estándar está orientado a electrónica de consumo, sistemas de audio especiales y equipos de video.

2.3 IrDA (para nuestro caso de redes inalámbricas se utilizara este estándar)

Los datos transmitidos pueden ser codificados de 2 formas diferentes. Hasta una tasa de transmisión de datos de 4 Mbps se utiliza la codificación RZI, mientras que para una tasa de transmisión superior a la anterior se utiliza el esquema de modulación 4PPM.

3.3.2 Bluetooth

Bluetooth incorpora varios mecanismos de seguridad que hacen de esta tecnología una de las más seguras de todo el mercado. Se definen mecanismos de seguridad respecto a 2 capas de protocolo:

1. Seguridad a nivel de banda base

Explicaremos ahora, pero en términos de seguridad, como se establece una piconet.

Durante el establecimiento de la conexión en una piconet el maestro crea una tabla de carácter pseudoaletaorio con la secuencia o patrón de saltos de frecuencia que deben utilizar todos los dispositivos que permanezcan a la piconet durante el transcurso de las comunicaciones. Al establecerse la conexión el dispositivo esclavo recibe un paquete FHS que le permite el poder sincronizar su reloj interno con el reloj del maestro, ya que los relojes de cada dispositivo funcionan con independencia de los demás, y por tanto se hace necesario el coordinar todos estos. Cabe decir que a lo largo de la comunicación se tendrán que actualizar periódicamente dichos relojes.

2. Seguridad a nivel de enlace

En el nivel de enlace se distinguen 3 tipos diferentes de mecanismos de seguridad:

2.1 Autenticación

La autenticación es el proceso donde un dispositivo verifica su identidad en otro dispositivo para poder acceder a los servicios que este ofrece. El proceso de autenticación no precisa la intervención directa del usuario, implicando entonces un esquema de desafío/respuesta entre cada par de dispositivos que emplea una clave de enlace común de 128 bits.

Cuando dos dispositivos se intentan comunicar por primera vez entre ellos se utiliza lo que se conoce como “pairing”. El pairing es un procedimiento de inicialización para crear una clave común entre dos dispositivos de forma segura, consiguiendo con esto que para posteriores comunicaciones entre ambos dispositivos los dos se reconozcan mutuamente como dispositivos seguros.

2.2 Autorización

La autorización es el procedimiento donde se determina el nivel de derechos que tendrá cierto dispositivo Bluetooth respecto a los servicios ofrecidos por un sistema. Se pueden distinguir 3 tipos de niveles:

-Derecho total: el dispositivo puede acceder sin ningún tipo de restricción a cualquier servicio que quiera.

-Derecho parcial: el dispositivo posee una confianza limitada, pudiendo acceder tan solo a unos servicios específicos.

-Derecho nulo: el dispositivo no puede acceder absolutamente a ningún servicio ofrecido por el sistema.

2.3 Cifrado de datos

El cifrado de datos como bien su nombre indica será el mecanismo encargado de cifrar la información que se envié entre los dispositivos Bluetooth. Este mecanismo es completamente opcional, aunque siempre será muy conveniente usarlo.

3.3.3 Tercera generación/3G

Respecto a los mecanismos de seguridad se distinguen principalmente 5 de estos:

1. Seguridad de acceso a la red

La seguridad de acceso a la red son el conjunto de características de seguridad que proporciona a los usuarios acceso seguro a los servicio ofrecidos por 3G, así como también protege contra ataques al enlace de acceso vía radio. Sus principales características son: confidencialidad de la identidad del usuario, autenticación de entidad, confidencialidad de los datos, integridad de datos e identificación del equipo de usuario.

2. Seguridad del domino de red

La seguridad del dominio de red se basa en un serie de características las cuales tienen como función la de permitir a los nodos del dominio del proveedor intercambiar de forma segura datos de señalización.

En este nivel de seguridad se llevan a cabo los siguientes procesos:

- Autenticación de entidad.
- Negociación de claves.
- Distribución de claves.
- Confidencialidad de datos.
- Integridad de datos.
- Detección de fraudes.

Los primeros 5 procesos enunciados son los que permiten a los diferentes nodos del dominio del proveedor autenticar de forma segura y negociar las claves de sesión, para que justamente después intercambiar de forma segura los datos de señalización.

3. Seguridad del dominio de usuario.

La seguridad del dominio de usuario son el conjunto de mecanismos y características que se encargan de hacer seguro el acceso a la estación móvil. Se identifican los siguientes mecanismos o características:

- Autenticación usuario-USIM.
- Autenticación USIM-UE.

4. Cuarto mecanismo: Seguridad en el nivel de aplicación.

Este nivel de seguridad está formado por el conjunto de mecanismos y características que permiten a las aplicaciones del dominio de usuario y del dominio del proveedor intercambiar mensajes de forma segura. Se incluirán por tanto:

- Mensajes seguros entre USIM y red.
- Confidencialidad de tráfico de usuario en la red.

5. Quinto mecanismo: Visibilidad de seguridad y configurabilidad

Los mecanismos de seguridad deberán ser aplicados de una forma transparente al usuario, aunque a petición de este el sistema tendrá que notificar los siguientes aspectos: el cifrado de la red de acceso, el cifrado de toda la red y el nivel de seguridad 2G/3G.

Por otro lado la configurabilidad es la capacidad de configurar ciertos servicios como por ejemplo: Habilitar/inhabilitar la autenticación usuario/USIM para ciertos servicios, aceptar/rechazar llamadas no cifradas entrantes, establecer o no llamadas no cifradas y aceptar/rechazar el uso de ciertos algoritmos de cifrado.

3.3.4 Wifi

Analizaremos a continuación los diferentes métodos de seguridad que utiliza Wifi.

1. Filtrado de direcciones MAC

El filtrado de direcciones consiste en suministrar a cada punto de acceso un listado de las diferentes MAC de los equipos que están autorizados a conectarse.

La ventaja principal es por tanto que ningún equipo, como por ejemplo un equipo malicioso, que no esté incluido en la lista de direcciones no podrá conectarse.

2. Protocolo de seguridad WEP

WEP o Wired Equivalente Privacy es el algoritmo opcional de seguridad para ofrecer protección a las redes inalámbricas incluido en la primera versión del IEEE 802.11.

El estándar 802.11 ofrece mecanismos de seguridad mediante procesos de autenticación y de cifrado. En el modo Ad Hoc la autenticación puede realizarse mediante un sistema abierto o mediante un sistema de clave compartida. Un punto de acceso que reciba una petición podrá conceder autorización a cualquier estación o solo a aquellas que estén permitidas. Como bien hemos visto en un sistema de clave compartida tan solo aquellas estaciones que posean una llave cifrada serán autenticadas.

El protocolo WEP utiliza el algoritmo RC4, que es utilizado para cifrar las transmisiones que se realicen a través del aire. Además también emplea el algoritmo de comprobación de integración CRC-32, el cual se emplea para proteger el texto cifrado con anterioridad frente a posibles modificaciones no deseadas por parte de atacantes.

3. VPN

El VPN es una herramienta para proteger las comunicaciones. Las VPN crean un túnel criptográfico entre 2 puntos determinados, utilizando para esto encriptación mediante el protocolo IPSEC.

El origen de este se remonta a cuando se empezó a tomar conciencia de la fragilidad en la seguridad Wifi debido a las carencias y fallos de WEP, donde en algunos sectores se difundió su uso con el fin de mejorar y reforzar la encriptación. Básicamente lo que hace el VPN es crear un túnel entre el cliente y el servidor, quedando de esta manera protegida la conexión con IPSec, el cual es un método de encriptación muy robusto.

4. WPA

Implementa la mayoría de lo que conforma el estándar IEEE 802.11i y fue diseñado para funcionar con todas los dispositivos de redes inalámbricas, excepto con los puntos de acceso de primera generación. Los datos utilizan el algoritmo RC4 con una clave de 128 bits y un vector de inicialización de 48 bits. Una de las mejoras más sobresalientes sobre su predecesor (WEP) es TKIP (Temporal Key Integrity Protocol, o Protocolo de integridad de clave temporal), el cual consiste en el cambio dinámico de clave mientras se utiliza el sistema.

Además de proporcionar autenticación y ciframiento WPA proporciona mejor integridad de la carga útil. WPA utiliza un Código de Integridad de Mensaje (MIC o Message Integrity Code) que es en realidad un algoritmo denominado. El Código de Integridad de Mensaje de WPA incluye un mecanismo que contrarresta los intentos de ataque para vulnerar TKIP y bloques temporales. WPA incluye las siguientes tecnologías: IEEE 802.1x, EAP, TKIP, MIC o Michael.

5. WPA2

WPA2 es el nombre dado por la Wifi Alliance a la segunda fase del estándar IEEE 802.11i. La seguridad es mucho más fuerte y robusta en comparación con el protocolo WPA. WPA2 ya no se basa en un parche temporal sobre el algoritmo RC4 sino que utiliza el algoritmo de encriptación AES. Dicho algoritmo requiere un hardware mucho más robusto que los anteriores protocolos por lo que algunos puntos de acceso antiguos no pueden utilizar dicho protocolo.

La implementación de protección que se aplica en el estándar de seguridad Wifi 802.11a se conoce con el acrónimo CCMP y está basada en el algoritmo AES. El cifrado que se utiliza es una cifrado simétrico de 128 bits y el vector de inicialización tiene una longitud igual que en el WPA, es decir de 48 bits.

3.3.5 Wimax

Wimax define en su pila de protocolos una subcapa de seguridad dedicada específicamente a proporcionar privacidad, confidencialidad y autenticación a todo usuario que desee utilizar la red. La tecnología Wimax basa su sistema de seguridad en los principios de autenticación y cifrado, los cuales hacen de ella actualmente una tecnología muy difícil de vulnerar. Más adelante cuando analicemos los ataques más comunes que suelen recibir Wifi y Wimax nos

daremos cuenta como Wimax prácticamente no recibe ataques en comparación con Wifi. Esto en otras cosas es debido a la gran seguridad que implementa.

1. Autenticación

La autenticación sirve para garantizar el acceso seguro a la red y por consiguiente para evitar que usuarios no deseados o no autorizados puedan entrar o hacer uso de ella, identificándose dos tipos diferentes:

1.1 OSA: en este método de autenticación el cliente realiza una solicitud de autenticación asociada a su propia dirección MAC, a lo que sigue una respuesta de la estación base. Dicha respuesta contendrá la aceptación o denegación de la solicitud por parte de la estación base.

1.2 SKA: este proceso se basa en las claves compartidas que ambos extremos deberán conocer. Cuando un usuario quiera conectarse a una red que ya conoce ambos extremos deberán intercambiarse las claves compartidas, donde en el caso afirmativo la estación base tendrá que permitir de forma obligada el acceso del usuario a la red.

2. Certificado digital X.509

El certificado digital es lo que utiliza el estándar 802.16 para realizar la autenticación de estaciones de usuario. A través de este documento digital una autoridad de certificación garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública. Existen varios formatos para estos certificados, siendo uno de ellos el IT-T X.509.

La estructura de un certificado X.509 es la siguiente:

- Certificado.
    - Versión.
    - Número de serie.
    - ID del algoritmo.
    - Emisor.
    - Validez.
        - No antes de.
        - No después de.
    - Tema.
    - Tema información de clave pública.
        - Algoritmo de clave pública.
        - Tema clave pública.
    - Identificador único de emisor (opcional).
    - Identificador único de tema (opcional).
    - Extensiones (opcional).
- Algoritmo de certificado de firma.
- Certificado de firma.

3. Cifrado

Después de que la estación base autorice a la estación de usuario son necesarios también mecanismos de cifrado para poder así velar por la confidencialidad y la integridad de los datos. Para hacer esto posible la estación del usuario envía a la estación base una solicitud de claves de cifrado llamadas TEKs, las cuales son enviadas por la estación en un mensaje de respuesta. A su vez estos mensajes están cifrados por una clave conocida por ambos extremos.

Los algoritmos utilizados para el cifrado pueden ser: 3DES, AES y RSA.

Una vez conocidas las TEKs se pueden usar diferentes técnicas para cifrar los datos: CBC (DES), CBC (AES), CTR (AES) y CCM (AES).

4. Seguridad añadida por la propia arquitectura Wimax

Además de todo lo anteriormente dicho el propio diseño de la tecnología Wimax juega un gran papel en cuanto a cuestiones de seguridad:

-Wimax se diseñó como una tecnología MAN/WAN de operador la cual tiene que poder interconectar muchos usuarios. Al ser una red orientada a una gran escala la propia tecnología se diseñó para poder velar por la seguridad con total garantía.

-El acceso al medio no es ni mucho menos aleatorio, sino que es completamente determinista y está regido por una estación base que actúa en todo momento como árbitro controlando las transmisiones. Ningún terminal no autorizado puede transmitir datos de forma indiscriminada hacia la estación base o hacia otras estaciones de usuario.

5. AES

Advanced Encryption Standard (AES) se basa en el algoritmo de Rijindael, que es un método de cifrado de bloques con fuertes propiedades criptográficas. Además de ofrecer una fuerte encriptación AES es rápido, fácil de implementar en hardware o software, y requiere menos memoria otros esquemas de cifrado comparables. La eficiencia computacional de AES ha sido una razón clave para su rápida adopción generalizada. El algoritmo estándar de cifrado avanzado AES funciona con un tamaño de bloque de 128 bits de los datos, organizados en una matriz de 4 x 4 de bytes llamado estado. Los tamaños de las claves de cifrado pueden ser 128, 192 o 256 bits de longitud aunque la tecnología Wimax especifica el uso de claves de 128 bits.

6. 3DES

Este algoritmo y sobre todo en aplicaciones WIMAX está desapareciendo poco a poco, siendo sustituido por el algoritmo AES. No obstante explicaremos brevemente este:

En criptografía el Triple DES se llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, el cual fue desarrollado por IBM en 1978.

7. RSA

El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques que utiliza una clave pública, la cual se distribuye, y otra privada, que es guardada en secreto

por su propietario. Cuando se envía un mensaje el emisor busca la clave pública de cifrado del receptor y una vez que dicho mensaje llega al receptor éste se ocupa de descifrarlo usando su clave oculta.

Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado. Emplea expresiones exponenciales en aritmética modular.

La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales.

3.4 Ataques y recomendaciones de seguridad

Vamos a ver a continuación los diferentes ataques que pueden afectar a cada una de las tecnologías estudiadas, así como las correspondientes recomendaciones de seguridad.

3.4.1 Infrarrojos

En redes infrarrojas el ataque más común (prácticamente el único) que se realiza es el secuestro de la señal. El fin que tiene este ataque es el de robar información sensible, así como enviar por parte del atacante información maliciosa.

Para evitar este ataque simplemente hay que asegurarse que la señal no pueda escapar hacia ningún sitio no deseado. En el caso de que se tuviese constancia que la señal ha sido secuestrada bastaría con salirse de la red creada o interrumpir la emisión de la señal.

Damos los siguientes consejos en cuanto a seguridad:

1. En conexiones punto a punto, alinear y asegurarse de que se está transmitiendo al receptor deseado.

2. En caso de que nuestro receptor haya dejado de recibir la señal, dejar inmediatamente de emitir e intentar averiguar la causa.

3. Utilizar siempre codificación para todo tipo de transmisión.

4. Para conexiones tipo causi-difuso o difuso asegurarse que la señal no puede escapar hacia un sitio o lugar no deseado.

5. Asimismo y respecto al anterior punto, asegurarse de que en el espacio donde se esté llevando a cabo la conexión tampoco existe ningún dispositivo no deseado.

6. No transmitir información que se considere sensible en entornos no seguros.

3.4.2 Bluetooth

Dado que la tecnología Bluetooth es una tecnología la cual puede verse sometida a multitud de ataques diferentes, se verán a continuación los ataques más conocidos y más comunes que se puedan dar.

Bluesnarf

El atacante utiliza el OBEX Push Profile (OPP), originalmente desarrollado para intercambiar tarjetas de negocios y otros objetos, donde en la mayoría de los casos este servicio no requiere autenticación. El ataque BlueSnarf realiza una solicitud OBEX GET de nombres de archivo conocidos tales como telecom/pb.vcf (el directorio telefónico) o telecom/cal.vcs (el archivo calendario). Si el firmware en el aparato víctima se implementa de forma incorrecta, el atacante puede obtener acceso a todos los archivos del aparato víctima.

BlueSnarf++

El BlueSnarf++ le da al atacante un acceso de lectura/escritura total por medio del OBEX Push Profile. Si se está ejecutando un servidor de FTP OBEX en el aparato, se puede establecer una conexión por medio del servicio OBEX Push sin emparejamiento.

El atacante puede ver todos los archivos en el sistema de archivos (utilizando el comando 1s) e inclusive borrar archivos (el comando rm). Asimismo el atacante también puede realizar acciones en cualquier memoria instalada en el aparato, incluyendo tarjetas de extensión de memoria tales como Memory Stick o tarjetas SD.

Bluebug

Tiene como fin el ejecutar comandos maliciosos AT en el terminal; extraer información sensible; modificar datos, contactos o notas; enviar mensajes desde el dispositivo victima e incluso provocar que la víctima haga llamadas no deseadas. El atacante intenta establecer una conexión RFCOMM, para que a través de esta intentar ejecutar los comandos maliciosos.

Hellomoto

Este ataque explota el procesamiento incorrecto del manejo de aparatos confiables de algunos teléfonos Motorola. El atacante inicia una conexión utilizando el OBEX Push Profile y simula el envío de una vCard. Entonces el proceso de envió se interrumpe, pero el aparato del atacante permanece en la lista de aparatos confiables en el teléfono de la víctima. Utilizando esta entrada a la lista de aparatos confiables el atacante puede conectarse al perfil del teléfono sin autenticación. Una vez que se establece una conexión el atacante puede tomar control del aparato utilizando comandos AT.

Blueline Attack

A través de un mensaje por pantalla, el cual puede parecer totalmente verídico y coherente, se intenta engañar al usuario para que acepte este mensaje. Lo que pasa en realidad es que el usuario no está aceptando lo que supuestamente le está diciendo el mensaje, sino que al aceptar habrá aceptado en realidad a ese atacante en su lista de confianza. Una vez dentro del terminal el atacante ya estará en disposición de poder ejecutar comandos maliciosos.

Blue MAC Spoofing

Su objetivo será acceder a servicios no autorizados y el robo de información, donde para ejecutar dicho objetivo el atacante suplantara la dirección MAC de un dispositivo de confianza. Una vez suplantada está el atacante utilizara sus credenciales para acceder a servicios que requieren autenticación y/o autorización.

Bluejackiing

El Bluejackiing no es en realidad un ataque como pueden ser todos los anteriores, ya que en realidad no persigue ningún fin estrictamente malicioso, sino que tan solo persigue el enviar imágenes, mensajes o contactos al dispositivo victima (mayormente con fines publicitarios). El modo de ejecución de este ataque es enviar mensajes de forma continua a todos los dispositivos Bluetooth activados y sin contraseña que estén en su radio.

The car Whisperer

Para llevar a cabo este ataque el atacante buscara en primer lugar un dispositivo el cual este en modo visible y que además no esté conectado actualmente con ningún otro. Cuando obtenga este dispositivo intentará conectarse con el mediante la inserción de las diferentes claves de acceso que las compañías asignan por defecto. En el caso de que la clave del dispositivo víctima no haya sido cambiada y siga teniendo la de defecto no tendrá problema alguno en conectarse con él, donde una vez conectado ya podrá tanto enviar como capturar audio.

Nombre: Headsets Hijacking

El modo de ejecución es exactamente igual al anterior ataque, a excepción de que aquí se querrá hackear el dispositivo de manos libres para auriculares. El atacante únicamente busca aquellos dispositivos que: estén visibles, no estén ocupados actualmente y que tengan una clave de fábrica. Si cumplen estos 3 objetivos tan solo deberá probar las diferentes claves por defecto hasta encontrar la que posea el dispositivo.

Cabe decir que en determinados modelos es posible incluso cortar un conversación en progreso e inyectar audio.

The Laptop Whisperer

Su objetivo será capturar o introducir audio en el ordenador de la víctima conectándose directamente al perfil de auriculares sin necesidad de ningún tipo de autenticación. El ataque es tan sencillo de llevar como parece, ya que existe un defecto en la pila de protocolos Widcomm.

BluePrinting

A través de la dirección MAC del dispositivo víctima el hacker querrá averiguar el fabricante y el modelo del dispositivo. Esto es posible ya que la dirección MAC, compuesta de 6 bytes, indicara en los 3 primeros el nombre del fabricante y en los 3 últimos el modelo del dispositivo.

BlueSmack

El BlueSmack es un ataque DoS que puede ser realizado utilizando herramientas estándar que son transportadas con Bluez Linux, el cual es muy similar a un ataque bien conocido que fue utilizado para atacar las primeras versiones del Windows 95 de Microsoft.

Al igual que el ping ICMP, la idea del ping L2CAP es también comprobar la conectividad y medir el tiempo de retorno en un vínculo establecido. Con la ayuda de la herramienta 12ping que se transporta con el distributivo BlueZ estándar el usuario puede especificar la extensión de los paquetes a ser enviados. Para lograr el resultado deseado puede usarse la opción -s para especificar un tamaño de aproximadamente 600 bytes.

BlueSpam

El método de ejecución está basado simplemente en buscar dispositivos con el Bluetooth activado al cual se le puedan mandar determinados mensajes.

Denegación de servicio mediante envío masivo

Bluetooth es susceptible a los ataques de denegación de servicio a través del envío masivo de mensajes. No obstante este tipo de ataques no son significativos y son muy fáciles de evitar, puesto que tan solo habrá que salirse del rango efectivo del dispositivo atacante.

Fuzzing

El ataque Fuzzing consiste en el envío de datos malformados o de datos no estándar hacia el dispositivo Bluetooth con el fin de ver cómo se comporta este. Si la respuesta del dispositivo se hace más lenta o se detiene por estos ataques, quiere decir que existirá una grave vulnerabilidad en la pila de protocolos.

BlueChop

El propósito de este ataque es el de afectar una piconet establecida utilizando un dispositivo que no es parte de la red. Este ataque se basa en el hecho de que la unidad central soporta conexiones múltiples que pueden ser utilizadas para crear una red extendida (una scatternet). El atacante imita la dirección de un aparato al azar que es parte de la piconet y se vincula a la unidad central afectando a la piconet.

BlueBump

Está basado en la idea de establecer una conexión confiable con el aparato de la víctima lo cual se puede lograr enviando una tarjeta de contacto a fin de hacer que el receptor realice una autenticación. El atacante mantiene la conexión abierta pero le pide a la víctima que borre la clave de vínculo del aparato del atacante, aunque la víctima no es consciente de que la conexión aun esta activa. El atacante entonces solicita una regeneración de la clave de vínculo. Como resultado, el dispositivo atacante obtiene una nueva entrada en la lista sin autenticación, teniendo este por consiguiente acceso al dispositivo victima hasta que se borre la clave.

PIN-Crack

Consiste en deducir un código PIN de un dispositivo, pudiéndose hacer de dos formas:

Pasivo por Spoofing: se sustituye a un dispositivo y esperamos a que la víctima cliente se conecte a nosotros e introduzca el PIN.

Activo: consiste en hacer fuerza bruta y probar PINs desde 0000 hasta 9999.

NastyVCard

Algunos dispositivos tiene un parche XML mal programado, donde esto puede permitir provocar segmentaciones o ejecución de código en el parcheo de VCARDs. También se pueden usar las VCARDs para enviar mensajes (BlueJack) ya que algunos dispositivos aceptan el vCard sin preguntar al usuario.

Por tanto y en vista de todo lo anteriormente visto ofrecemos una serie de consejos para intentar garantizar la seguridad de nuestro dispositivo Bluetooth y evitar los ataques anteriores:

1. Activar el Bluetooth únicamente cuando se vaya a utilizar.
2. No aceptar nunca ninguna conexión desconocida.
3. Utilizar siempre que se pueda el método de cifrado para las conexiones.
4. Otorgar un nombre a nuestro dispositivo el cual no refleje ningún aspecto sobre el dispositivo en si, como por ejemplo el modelo o la marca.
5. Revisar periódicamente la lista de dispositivos que tengamos agregados en nuestra lista de confianza.
6. Mantener siempre actualizado nuestro dispositivo.
7. Utilizar siempre clave de acceso.
8. Asimismo no utilizar nunca una clave que venga por defecto, como tampoco una clave sencilla y predecible. Para crear una contraseña fuerte se recomienda alternar entre caracteres, símbolos y números, así como también entre minúsculas y mayúsculas. No obstante debemos asegurarnos que podremos recordarla en un futuro.
9. Configurar nuestro dispositivo para que no resulte visible a los demás.
10. Evitar guardar por si acaso datos, imágenes u otros archivos delicados en nuestro teléfono.
11. Cambiar la configuración predeterminada del dispositivo Bluetooth respecto al uso que se le vaya a dar a este.
12. Configurar el dispositivo con el nivel justo de energía, con el fin de que las transmisiones se mantengan dentro de un perímetro de seguridad muy pequeño.
13. Utilizar siempre que se pueda (esto variara según la versión utilizada) el modo máximo de seguridad, es decir el nivel 3 (seguridad a nivel de enlace).
14. Utilizar el cifrado de enlace en absolutamente todas las conexiones.

15. En caso de que se esté utilizando una comunicación multi-hop asegurarse de que todos los dispositivos cuentan con cifrado.

16. Tener especial cuidado con quien aceptamos en nuestra lista de confianza.

17. Asegurarse de que la autenticación mutua se llevó a cabo en todas las comunicaciones.

18. Habilitar el cifrado para todas las conexiones de radiodifusión.

19. Configurar el tamaño de clave de cifrado a lo máximo permitido (128bits).

20. Implementar plantillas de usuario de autenticación, como la biometría, tarjetas inteligentes o la infraestructura de clave pública (PKI).

21. En el caso de perder o de ser robado un dispositivo Bluetooth los usuarios deben desvincular inmediatamente el dispositivo que falta en el resto de dispositivos Bluetooth con el que fue emparejado previamente.

22. Instale software antivirus en dispositivos Bluetooth que soporten este tipo de software.

23. Mantener al día los parches de firmware y las actualizaciones.

24. Asignar autenticación obligatoria a todas las conexiones entrantes.

25. Restringir el acceso de comandos AT desde el interfaz Bluetooth.

26. Rechazar cualquier mensaje, imagen o petición que parezca mínimamente sospechosa.

27. Aceptar intercambio de información únicamente con usuarios que tengamos la plena certeza que son fiables.

28. En el caso del ataque de denegación de servicio bastara con salir del rango efectivo del dispositivo atacante.

29. Utilizar en la medida de lo posible claves PIN de longitud extensa, hasta 16 bytes.

30. No permitir el acceso a archivos compartidos de nuestro dispositivo. Asimismo tampoco será recomendable el tener información sensible en esta sección.

3.4.3 Tercera generación/3G

Los ataques que más comunes que se suelen ejecutar sobre redes 3G son los siguientes:

Robo de datos masivos

Este ataque es uno de los más potentes actualmente. Consiste básicamente en robar todo tipo de información sensible acerca de cientos o miles de personas, pudiendo ser esta información personal o bancaria. Para este ataque no hay en realidad protección posible que esté en nuestras manos, ya que la seguridad de los datos no depende de los usuarios sino de las propias compañías.

Ataques a la banda base

Su método de ataque es generar un error de desbordamiento en el código que gestiona la pila de protocolos de comunicaciones, con el fin de poder introducirse en el dispositivo y ejecutar código malicioso.

Ataque criptográfico

El ataque criptográfico consiste en romper o destruir un mecanismo de cifrado, siendo el más claro ejemplo de esto la destrucción del algoritmo KASUMI en 2010 por un grupo de investigadores. Este algoritmo es el algoritmo empleado de cifrado utilizado por los móviles 3G, el cual fue destruido tan solo en 2 horas y a través de un PC estándar.

Malware engañoso

El malware no es un tipo tan directo de ataque como pueden ser otros. Este ataque o malware puede estar presente en muchos sitios y a través de diferentes formas como: correos, páginas webs, aplicaciones, enlaces, programas, entre otros.

Ataque a vulnerabilidades de protocolo

Este ataque intenta acceder a un dispositivo a través de las vulnerabilidades que puedan existir en este, más concretamente para que el ataque sea efectivo no deberá existir autenticación de red y que además el móvil este cifrando los datos.

Captura de identidad pasiva.

Un ataque pasivo utiliza una MS modificada y explota la debilidad por la cual la red solicita al usuario que envíe su identidad en texto claro.

Captura de identidad activa

Utilizando una BS vulnerada este ataque explota una vulnerabilidad de la solicitud red, donde la MS envía su identidad de usuario permanente en texto claro. Para hacer esto el intruso atrae al usuario para que se conecte a la falsa BS con la intención de pedirle posteriormente su identidad de usuario permanente en texto claro, poniendo como escusa un nuevo registro o un desajuste de identidad temporal debido a un problema en la base de datos.

Signaling DOS

Este ataque finaliza sesiones móviles activas en la red. Comprende el envío de pequeñas cantidades de datos para reiniciar una sesión después de que ésta haya sido liberada. El

ataque de bajo volumen puede crear congestión en el controlador de radio de la red (RNC), donde el sobrecargar el RNC repercute en una denegación de servicio para el usuario.

Battery Drain

Al igual que el anterior ataque este también afecta a las sesiones activas. Su método de ejecución es enviar paquetes a un dispositivo móvil para evitar que éste entre en modo suspenso. El ataque puede constar de algo tan ínfimo como enviar 40 bytes cada 10 segundos, lo que repercutirá en un consumo de recursos de radio y un agotamiento prematuro de las baterías de los dispositivos.

Ataque de redirección

En este ataque un atacante posee un dispositivo que puede hacerse pasar simultáneamente tanto por el subsistema de estación base (BSS) como por la MS. Para engañar a la víctima MS el atacante se hace pasar por un BSS legítimo mediante la difusión de un BSS ID falso. El atacante se conecta a otra red extranjera legal en nombre de la legítima MS y construye un túnel transparente para transmitir mensajes entre la red extranjera autorizada y la víctima MS. Dado que las claves AUTN, RAND se negocian con éxito, la víctima MS entonces será autenticada por la red exterior.

Suplantar BS / MS

El atacante utilizando un BS / MS se posiciona entre la SN y el usuario de destino. La protección de la integridad de los mensajes de señalización críticos protege contra la denegación de servicio a un cierto grado, ya que el intruso no puede modificar mensajes de señalización. Sin embargo, el sistema no impide que el atacante retransmita mensajes entre la red y el usuario de destino.

Damos los siguientes consejos en cuanto a seguridad:

1. Nunca abrir ningún tipo de correo o programa sospechoso.

2. No introducir datos sensibles (personales y bancarios) en ningún sitio, con la excepción de que sea un sitio oficial, obligatorio y tengamos la plena certeza de que es seguro.

3. Especial cuidado al descargar aplicaciones. No porque se puedan descargar determinadas aplicaciones ya implicara que son seguras o que son realmente lo que prometen (como por ejemplo el caso de Mooncraft).

4. Instalar antivirus. Los antivirus ya no son solo para ordenadores sino que también podremos encontrar antivirus para todo dispositivo que implemente 3G, como móviles o tablets. El tener instalado un antivirus nos reportara los siguientes beneficios:
    a. Protegernos de aplicaciones maliciosas.
    b. Opciones de control remoto en caso de pérdida o robo del dispositivo.
    c. Protección antispam.

   d. Filtrado de contenido.
   e. En caso de que nuestro dispositivo haya sido rooteado el antivirus nos dará la opción de crear un cortafuegos, con el fin de poder defendernos de posibles ataques de hackers.

5. Actualizar el dispositivo. Es muy recomendable el actualizar nuestro dispositivo móvil con regularidad, ya que al actualizar este podremos descargarnos los últimos avances en cuanto a seguridad.

6. Contraseñas. Ya sea para acceder al menú de inicio de nuestro teléfono como al correo, redes sociales, entre otros será muy recomendable en poner una contraseña de cierta dificultad y no una contraseña fácilmente predecibles o muy corta. Para la creación de contraseñas el mejor truco es alternar tanto en caracteres y números, así como en minúsculas y mayúsculas.

7. Paginas o enlaces sospechosos. Toda página que contengan malware podrá afectarnos de igual manera ya sea una Tablet, un PC o móvil de última generación por lo que deberemos tener especial cuidado con las páginas que parezcan sospechosas.

8. Trafico de red y conexión. Para el tráfico de red se recomienda la activación de protocolos de cifrado siempre y cuando sea posible. Asimismo si utilizamos un punto de acceso que no sea la red 3G, como por Wifi, deberemos asegurarnos que ese punto de acceso sea totalmente seguro.

9. Destrucción de datos. Un aspecto que puede resultar muy útil (no todos los dispositivos 3G lo implementan) es la destrucción de todos los datos de nuestro dispositivo tras introducir un número excesivo de contraseñas errores, como por ejemplo tras 15 o 20 intentos.

10. Establecer copias de seguridad. El realizar una copia de seguridad nos garantiza el poder recuperar el entorno y la información de nuestro dispositivo 3G exactamente a como estaba cuando se realizó dicha copia.

11. Conectar únicamente el GPS cuando se vaya utilizar. Recientemente se han registrado varios casos de fallos en la tecnología GPS, dando la oportunidad a un atacante de poder rastrear y seguir tu dispositivo.

12. Cifrado de datos en niveles superiores. El cifrar nuestros datos nos permitirá estar más protegidos frente a posibles amenazas. Para cifrar estos datos podemos usar protocolos como el HTTPS, SSH o el IPSEC.

13. Instalar y configurar un cortafuegos. El tener un cortafuegos bien actualizado y configurado evitara muchas intrusiones no deseadas, así como nos protegerá de otros muchas amenazas.

14. Utilizar el cifrado de voz Encrypti. Este cifrado permite cifrar las conversaciones telefónicas.

15. Usar aplicaciones para la protección de datos. Con el uso de estas aplicaciones se lograra incrementar aún más el nivel de seguridad.

16. Verificar conexiones. Se hace indispensable el verificar que el dispositivo al que vamos a conectarnos está totalmente limpio y libre de posible malware malicioso.

17. Usar VPN. Las conexiones VPN no solo estarán disponibles para las tecnologías Wifi y Wimax, sino que también podremos hacer uso de ellas en dispositivos 3G.

18. Cifrar todos los archivos del teléfono y de la propia tarjeta. Con este método se impide que toda persona que no conozca la contraseña maestra pueda ver cualquier tipo de archivo del teléfono.

19. Desactivar Wifi al no estar utilizando este. Asimismo asegurase siempre de estar conectados a un punto de acceso legítimo.

20. Configurar plenamente el dispositivo 3G utilizado respecto a las medidas de seguridad ofrecidas por este (no todos los dispositivos ofrecen la misma seguridad).

3.4.4 Wifi

Los ataques Wifi más comunes que se han podido identificar son los siguientes:

Romper claves WPE

Como bien se ha dicho a lo largo del proyecto el protocolo de seguridad WEP es totalmente inseguro en cuanto a seguridad. Hay principalmente dos métodos de romper la seguridad en este protocolo y por consiguiente obtener su clave, mediante fuerza bruta y mediante crackeo.

El método de fuerza bruta consiste tan solo en ir probando una tras otra posibles combinaciones de claves hasta dar con la correcta. Cabe decir que este método además de poder ser poco efectivo es muy lento.

El otro método, el método de crackeo, averigua la clave aplicando el proceso de cracking a un conjunto de paquetes #data capturados previamente. Para capturar esto paquetes se suele inyectar paquetes ARP con el fin de que se genere movimiento de tráfico en la red y poder así hacer una mayor captura de paquetes.

Romper claves WPA

La ruptura de claves WPA se basa en dos pasos, capturar el handshake y el crackeo mediante diccionario.

Cada vez que un cliente se conecta a una red con cifrado WPA, envía un paquete-saludo, o Handshake al AP al que se va a conectar, donde este paquete-saludo contiene la contraseña encriptada que se desea obtener.

El handshake solo se puede capturar exclusivamente cuando un cliente se conecta al punto de acceso. Por tanto se abren dos posibilidades, esperar pacientemente a que el cliente se desconecte y se vuelva a conectar, o bien, forzar la desconexión del cliente utilizando un ataque de desautenticación (es esto último lo que siempre se suele hacer).

Una vez obtenido el handshake (no se suele obtener a la primera por lo que es muy probable que se tenga que intentar varias veces) tan solo quedara crackear este mediante un diccionario. No obstante no basta con utilizar cualquier diccionario, ya que cuanto más tamaño y combinaciones tenga el diccionario más posibilidades habrá de encontrar la clave buscada.

Espionaje/Surveillance

El ataque de espionaje es sin duda la técnica más simple a la que se puede someter una red sin hilos. Consiste en observar el entorno para así recopilar información relacionada con la topología de red, pudiéndose utilizar esta información para posteriores ataques. En este caso y a diferencia de todos los demás ataques que vamos a ver a continuación, el ataque de espionaje es el único que no necesita ningún tipo de hardware o software, puesto que tan solo se necesita tener acceso a la instalación.

Mediante esta técnica el atacante puede encontrar información de gran valor a la hora de realizar un ataque, como por ejemplo la localización de las antenas, puntos de accesos, topología, etc.

Escuchas/Sniffing

El objetivo de las escuchas es monitorizar la red con el fin de capturar información sensible como por ejemplo, la dirección MAC o IP origen y destino, contraseñas, claves, identificadores de usuario, etc. Las escuchas se consideran un paso previo a ataques posteriores, como por ejemplo la inyección y modificación de paquetes sin necesidad de descifrar claves.

No obstante para que un dispositivo tenga la capacidad de llevar a cabo escuchas de red debe tener instalada o integrada una tarjeta WLAN que actué en modo promiscuo o en modo monitor, ya que estos modos de operación permiten recibir todo el tráfico que circula por la red. Adicionalmente es necesario utilizar un software especial llamado sniffer, el cual es un programa que se emplea para monitorizar toda la información que viaje a través de una red.

Denegación de servicio, clases principales.

Los DoS son uno de los tipos de ataques más sencillos de llevar a cabo y a la vez uno de los más complicados de contrarrestar. La Dos consisten básicamente en enviar un gran número de peticiones a un servidor de manera que los usuarios legítimos del servicio no puedan acceder a esos recursos.

Los principales ataques DoS son los siguientes:

- Ataque de inundación de buffer o Buffer Overflow
- Ataque de inundación de SYN o SYN Flood
- Ataque Teardrop
- Ping de la muerte
- Ataque de inundación ICMP
- Ataque Smurf

Denegación de servicio por saturación de ruido

EL objetivo principal que persigue el hacker con este ataque es imposibilitar la comunicación usuario-punto de acceso a través de la degradación de la señal.

Para conseguir degradar la señal evidentemente el hacker no podrá distanciar el punto de acceso del usuario y ni tampoco podrá ir interponiendo obstáculos entre ambos. Recordemos que una señal Wifi se puede ver afectada por 3 factores principalmente: distancia, obstáculos e interferencias. Por tanto lo que hará el hacker será debilitar la señal mediante interferencias, provocadas estas por una cantidad intensa de ruido.

Denegación de servicio por torrente de autenticaciones

Para que se pueda dar este ataque se deben cumplir 2 condiciones, que se utilice el estándar 802.1x y el servidor RADIUS, y además que cada usuario que quiera acceder tenga que autenticarse previamente.

Básicamente consiste en el envío masivo y simultaneo de peticiones falsas por parte de un atacante, consiguiendo así que el servidor RADIUS se mantenga ocupado con este atacante y tenga que denegar por consiguiente el servicio a los otros usuarios (puesto que no podrá atenderlos).

Puntos de acceso no autorizados/Rouge APs

En el caso de que se consiga conectarse a la instalación física de una red WLAN este es uno de los ataques más peligrosos. Un Rogue AP es un punto de acceso que se conecta sin autorización a una red ya existente. Estos puntos de acceso no son gestionados por los administradores de red y es posible que no se ajusten a las políticas de seguridad de la red.

Es de esta forma por tanto cuando se abre una puerta a todo tipo de ataques indeseados y maliciosos, puesto que permite a cualquiera con una terminal WLAN conectarse a la red y vulnerar todos los mecanismos que se basan en el cifrado de información entre extremos.

Generalmente los Rogue APs suelen emitir con más potencia que los puntos de acceso legítimos con el fin de que los usuarios se conecten a ellos por defecto.

Spoofing

Un ataque de Spoofing tiene como función el suplantar validadores, credenciales o identificadores estáticos, es decir parámetros que permanecen invariables antes, durante y después de la concesión de un privilegio, una autenticación, etc. Varios de estos valores son

por ejemplo las direcciones IP, direcciones MAC, nombre de dominio, nombres de recursos compartidos y direcciones de correo electrónico.

Una forma de ejecutar este ataque es a través de redefinir la dirección física o MAC de la interfaz inalámbrica por una dirección MAC valida dentro del sistema atacado. Para hacer esto basta con emplear un sniffer que permita (ataque pasivo) capturar alguna MAC valida en el sistema, con el fin de suplantar posteriormente la dirección MAC capturada. Cabe decir que para utilizar dicha dirección MAC se tendrá que esperar a que el usuario propietario de la MAC se desconecte, aunque también se puede ejecutar un DoS contra el con el fin de expulsarlo de la red.

Man in the Middle

Basado en Spoofing el ataque MITH consiste en interponerse entre dos sistemas. En este ataque un atacante intercepta y modifica los datos de la comunicación para así suplantar la identidad de las entidades implicadas en la comunicación. Puede escuchar todos los mensajes intercambiados entre las partes e incluso modificarlos y volver a enviarlos, implicando esto que los extremos sigan creyendo que se están comunicando con el extremo legítimo.

Los entornos que operan sobre las redes locales facilitan la captura y redirección de sesiones ya que una estación inalámbrica que transmite no es capaz de detectar presencia alguna de estaciones adyacentes con la misma MAC o IP.

Secuestro de sesiones /Hijacking

Hijacking es una amenaza de seguridad que al igual que MITH está también se vale del Spoofing, aunque en este caso se intentara tomar una conexión existente entre dos dispositivos de usuario. Tras monitorizar la red el atacante puede generar tráfico que parezca venir de una de las partes constituyentes de la comunicación, robando así la sesión de los usuarios correspondientes.

A continuación se expondrán las recomendaciones de seguridad más importantes a la hora de trabajar con una red, donde además distinguiremos 3 posibles escenarios:

Recomendaciones generales para Wifi doméstico y equipo propio.

1. Instalar el punto de acceso lo más lejos posible de la calle y las ventanas.

2. Configurar la intensidad de la señal intentando que tengamos conexión en los sitios donde nos conectemos habitualmente, pero también procurando que esta no escape hacia el exterior.

3. Desconectar el router o deshabilitar la opción Wifi cuando no se utilice o se esté fuera de cada durante un tiempo prolongado.

4. Utilizar siempre el protocolo de seguridad WPA2 (AES). En caso de que el router este obsoleto utilizar el protocolo WPA.

5. No utilizar nunca el protocolo WEP, puesto que es totalmente inseguro.

6. Instalar con inmediatez las posibles actualizaciones de firmware que pueda sacar el fabricante.
7. Cambiar la contraseña por defecto del router. Asimismo crear una contraseña que no tenga nada que ver con el usuario y que se considere robusta y fuerte.

8. Cambiar el SSID por defecto y deshabilitar el broadcast del SSID. Un buen SSID es aquel que nos desvela ninguna pista acerca del propio usuario y que tampoco llama la atención del hacker.

9. Utilizar un filtrado MAC. Únicamente se permitirá la entrada a los ordenadores o dispositivos que sean propiedad del entorno donde este el router, como por ejemplo una casa o una pequeña oficina.

10. Instalar y configurar mediante iptables un cortafuegos. Personalmente se recomienda utilizar un DMZ o cortafuegos desmilitarizado.

11. Deshabilitar la asignación automática de direcciones IP mediante DHCP.

12. Utilizar software de detección de intrusos, como por ejemplo mod_security, nikto o Snort.

13. Instalar y configurar un buen antivirus. No obstante no basta con instalar el mejor de los antivirus, ya que también se debe procurar el mantener este totalmente actualizado.

14. Desactivar tecnologías que no se utilicen, como por ejemplo puede ser WPS.

15. Actualizar el firmware del router.

16. Limitar el número de IPs asignables.

17. Ocultar el SSID de nuestra red.

18. Desactivar el DCHP.

19. Utilizar un navegador de última versión y mantenerlo actualizado. Muchos de estos navegadores nos avisan cuando vamos a acceder a lugares potencialmente peligrosos.

20. Instalar las actualizaciones y parches de nuestro sistema operativo.

21. Comprobar con regularidad que dispositivos se encuentran conectados a nuestra red.

22. Asignar direcciones MACs a IPs de manera estática en el router.

23. Configurar el router de manera que solo se pueda controlar desde una conexión LAN y no a través de la red Wifi. Con esto se asegura que si alguien consigue entrar en la red no pueda modificar la configuración del router.

24. Limitar el número de conexiones del router con el fin de que no haya más de las que se necesiten.

25. Cambiar las claves con regularidad.

26. Intentar navegar por redes seguras. Se pueden identificar estas por un candado en la parte derecha de la barra del navegador o cuando http termina en “s” (https).

Recomendaciones generales para Wifi público y equipo propio.

1. Utilizar un cortafuegos debidamente configurado.

2. Apagar el receptor Wifi cuando no se esté utilizando la red. Aunque ya no estemos haciendo uso de internet nuestro dispositivo seguirá vinculado con el punto de acceso.

3. Cifrar todo tipo de archivo confidencial o que contenga información sensible.

4. No escribir información privada o sensible, como por ejemplo información bancaria o personal.

5. En caso de que sea imprescindible enviar información sensible asegurarse de que el sitio web receptor utiliza SSL (en caso afirmativo contara con un icono de candado en la esquina derecha de la barra del navegador o el nombre http terminara en s, es decir https).

6. Desactivar Wi-Fi Ad-hoc, con el fin de evitar que nuestro dispositivo se conecte a otro dispositivo que no conocemos.

7. Utilizar una red privada virtual o VPN.

8. Evitar las conexiones automáticas a redes Wi-fi, ya que si no se correría el riesgo de conectarse a red Wifi abierta que fuese maliciosa.

9. Instalar y configurar debidamente un antivirus.

10. Desconfiar de posibles descargas de aplicaciones Wifi. Estas aplicaciones suelen ser programas maliciosos.

11. No usar la misma contraseña en diferentes sitios, puesto que si una persona obtuviese esta contraseña podría entrar en varios sitios y no solo en uno.

12. Instalar programas opcionales de cifrado. Estos programas aumentan la seguridad de manera que obligan a cifrar todos los datos que se envíen (Force-TLS y HTTPS-Everywhere).

13. Desactivar la opción de compartición de archivos.

14. Utilizar autenticación de dos pasos, siendo esta mucha más segura que la autenticación por contraseña única.

Recomendaciones generales para Wifi publica y equipo público.

1. Nunca y bajo ningún concepto guardar información que se pueda recordar. Es decir hay que deshabilitar la opción de recordar. Esto es muy común al acceder a redes sociales, correo u otras cuentas.

2. No escribir ningún tipo de información personal en el equipo. A no ser que sea extremadamente importante toda operación que contenga información sensible se recomienda hacerla desde un entorno más seguro.

3. Borrar el historial de navegación.

4. Tener cuidado con personas ajenas que puedan estar espiando nuestras acciones.

5. Usar páginas seguras con https.

6. Utilizar el teclado por pantalla.

7. No conectar nunca dispositivos de E/S en ordenadores públicos.

8. Asegurarse de haber cerrado toda sesión que se haya iniciado previamente.

3.4.5 Wimax

Analizaremos ahora los principales ataques que se suelen ejecutar contra redes Wimax.

Man in the middle o MITM

El ataque Man in the middle se refiere al tipo de ataque donde el atacante se entromete en la comunicación entre los puntos finales de una red con el fin de inyectar información falsa e interceptar los datos transferidos entre ellos. Este ataque es un tipo activo de espionaje en el que el atacante realiza conexiones independientes con las víctimas a través de mensajes entre ellos, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada cuando, de hecho, toda la conversación es controlada por el atacante. El atacante debe ser capaz de interceptar todos los mensajes que van entre las dos víctimas e inyectar nuevos.

Ataque a capa física Wimax mediante ruido RF

Una forma de conseguir denegar el servicio por parte de la estación base es evitar que esta transmita. Al igual que se vio en los ataques Wifi, Wimax también puede sufrir una ataque de bloqueo, generado este por una fuente de ruido muy fuerte. La intención de esta fuente de ruido es básicamente provocar la degradación de la señal y reducir la capacidad del canal con el fin de que las estaciones de usuario no puedan comunicarse con la estación base debidamente.

Ataque a estaciones base

El ataque a estaciones base se produce cuando una estación atacante duplica una estación base legítima, aprovechándose para esto de un posible fallo de omisión de autenticación.

Todos los usuarios de la estación base atacada piensan que se están comunicando con ella misma y no con una estación base no legitima, repercutiendo en una perturbación del servicio, robo de información y suplantación de identidades.

El método exacto de ataque depende del tipo de red. Por ejemplo en una red Wi-Fi el atacante tiene que suplantar la identidad de un punto de acceso legítimo, para inyectar después los mensajes maliciosos cuando el medio está disponible. En una red Wimax, esto es más difícil de hacer ya que Wimax utiliza acceso múltiple por división del tiempo, obligando así al hacker a transmitir mientras que la estación base legítima está transmitiendo. Es decir el hacker tan solo podrá transmitir cuando la estación base legitima transmita mensaje.

Ataque a protocolo DES

El objetivo que persigue este ataque es el de capturar y modificar la información que se transmite en las redes Wimax. Wimax está configurado para transmitir de una forma segura, aunque recientemente se descubrió un aspecto muy importante en el protocolo de cifrado DES.

En realidad no se descubrió una vulnerabilidad en sí, sino que se descubrió que la seguridad de este protocolo se estaba quedando obsoleta respecto a la potencia de algunos ordenadores modernos. El motivo de esto es que pese a que DES es en parte muy seguro, algunos ordenadores modernos son capaces de romper este protocolo mediante el uso de fuerza bruta.

Denegación de servicio mediante packet scrambling

Otra forma de conseguir denegar el servicio es mediante la inserción de paquetes maliciosos o paquetes de aleatorización. Este ataque se produce cuando los paquetes de control de los tramos ascendentes y descendentes son capturados por un sniffer, modificados y enviados de nuevo a la red, aunque no es en realidad tan sencillo.

Como bien se sabe Wimax actúa por división de tiempo (TDD), es decir las señales se transmiten en unos determinados instantes de tiempo. Lo que hará el atacante será analizar la secuencia de tiempo para así poder saber cuándo transmitir los paquetes capturados e interrumpir así la conexión. Es decir el atacante capturara, modificara y reenviara paquetes de control tras haber estudiado la secuencia de transmisión con el fin transmitir a la vez que la estación legitima y poder interrumpir la señal.

Manipulación de mensajes de gestión

El objetivo de este ataque es utilizar mensajes de gestión y hacer creer a los usuarios que provienen de una estación legitima. Conseguido esto se podrá denegar al servicio a los usuarios indicando que se desconecten o indicándoles que envíen mensajes sucesivos con el fin de colapsar a la estación base legítima.

Espionaje

Este ataque está basado en las escuchas ilegales que se producen cuando un atacante utiliza un analizador de tráfico Wimax. El atacante puede monitorear el tráfico de mensajes de gestión para identificar los sistemas de cifrado, determinar la huella de la red o llevar a cabo el análisis de tráfico en relación con determinados nodos Wimax. Los mensajes de datos recogidos durante las escuchas también se pueden utilizar para descifrar el cifrado DES-CBC, sin embargo, AES proporciona una robusta confidencialidad, consiguiendo así proteger los mensajes de datos del espionaje.

Damos las siguientes recomendaciones de seguridad:

1. Asegurarse de que ninguna persona no autorizada acceda o trabaje con terminales Wimax. La tecnología Wimax se usa mayormente en entornos laborales por lo que esta medida se hace muy importante.

2. Configurar, sobre todo en entornos laborales, de una manera óptima la conexión Wimax asegurando y optimizando aspectos como autenticación, el control de acceso, la auditoria y la protección de la comunicación.

3. Utilizar cuando se requiera conexiones VPN.

4. Utilizar soluciones capaces de soportar el protocolo de autenticación extensible, EAP.

5. Utilizar siempre que se pueda tarjetas inteligente PKI, las cuales poseen ciertas características que las hacen muy óptimas en cuanto a seguridad.

6. Instalar y configurar un firewall. En otras funciones el configurar de manera correcta un cortafuegos garantizara una mayor protección contra posibles vulnerabilidades y amenazas.

7. Utilizar sistemas de prevención basados en host y sistemas de detección de intrusos. Estos sistemas alertaran frente a posibles intrusos, así como también informaran de cualquier anomalía, alteración o comportamiento inusual del sistema.

8. Utilizar antivirus y software antiespia. Estos programas ayudaran a prevenir la propagación de virus, gusanos y otros programas maliciosos entre los dispositivos conectados en red. La mayoría de los dispositivos cliente se encuentran en riesgo de amenazas de malware, por lo que estos dispositivos deben tener instalado un software antimalware adecuado y recibir actualizaciones automáticas.

9. Actualizar con regularidad los programas y sistemas instalados, así como el propio sistema, donde esto ayudara a mantener al día a nuestro equipo sobre las amenazas más actuales. Muchos vendedores suelen emitir parches, actualizaciones de firmware

y actualizaciones de software para corregir las vulnerabilidades de seguridad conocidas y hardware. Por tanto se debe consultar regularmente con los proveedores para identificar estos cambios y aplicar cuando sea necesario.

10. Desactivar Wimax siempre y cuando no se esté utilizando.

11. Utilizar autenticación mutua a través de IEEE 802.1x y un servidor RADIUS.

12. Utilizar un segundo canal de verificación, repercutiendo esto en tener una mayor seguridad a la hora de autenticar a un usuario.

13. Montar rutas ARP estáticas en los equipos que formen la comunicación.

14. En el caso puntual de utilizar SSH:

• No aceptar una nueva fingerprint si ya habíamos guardado la anterior. Ante un mensaje de este tipo lo más recomendable seria cancelar toda acción.

• Validar de forma local las fingerprint del servidor.

• Ante posibles alertas de cambios en certificados, cancelar la acción y revisar.

15. Considerar utilizar mecanismos extra como: autenticación mutua, reconocimiento de voz, infraestructuras de clave pública y exámenes de latencia.

16. Usar módulos criptográficos FIPS e implementación de cifrado.

17. Disponer de ciertas herramientas para la detección en caso de las tablas ARP, como por ejemplo ARPWATCH o ARPALERT.

18. Usar ciertos puglins para detectar posibles problemas, como por ejemplo search_promisc y scan_poisoner.

3.5 Software de intrusion y protección para Wifi y Wimax

- Distribuciones (solo Wifi)

Wifislax, Wifiway, Aircrack, NST, Backtrack, Operator, Pentoon, Ubuntu, STD, Helix, DVL.

- Antivirus

Gratuitos: Avast Free Antivirus, Avira AntiVir Free Edition, AVG Free, Microsoft Security Essentials, Panda Cloud Antivirus, BitDefender Free, Comodo Antivirus, ClamWin, Emsisoft a-squared Free.

De pago: Panda Software Antivirus, Kaspersky Antivirus, AVG Internet Security, Norton Antivirus, Eset Nod32 Antivirus, G Data Antivirus.

- IDS/Sistema de Detección de Intrusos

Gratuitos: Acidbase, Fcheck, Snort, Hunt, Prelude, Prevx Home, Foundstone Attacker, Foundstone Carbonite, SnootNetCop Standard.

De pago: Vortex IDS, Antiacker Haskery, ZoneAlarm.

- Programas para cifrar archivos

Gratutios: dirLock v1.4, MyLockBox v1.2, Sofonesia Folder Protector, Cryptainer LE, CryptArchiver Lite, SuperStorm, TrueCrypt.

De pago: Hide Folders, myWinLocker, Folder Guard, 7-zip.

- Cortafuegos

Gratuitos: Agnitum Outpost Free, Comodo Firewall, Zonealarm Free (se recomienda personalmente usar este), PC Tools Firewall Plus 7, AVS Firewall, Handycafe Firewall, Private Firewall, SoftPerfect Firewall, PeerBlock y Windows 7 Firewall Control.

De pago: ZoneAlarm Pro, Panda Firewall, Online Armor Premium, McAfee Internet Security Firewall, AVG, Eset, Trend Micro.

3.6 Simulaciones

El apartado de simulaciones corresponde con el apartado final de cada una de las redes estudiadas. En estas simulaciones se estudiara como configurar un dispositivo de una forma óptima en cuanto a seguridad, a excepción de la red Wifi donde además se han añadido varios ataques. Cabe decir que debido a la limitación impuesta en la memoria se hace totalmente imposible el representar estas simulaciones nuevamente, puesto que sobrepasarían ampliamente la cantidad de páginas máximas. No obstante explicaremos brevemente que se ha hecho en cada una de estas simulaciones:

No todas las recomendaciones de seguridad pueden ser aplicadas en todos los dispositivos, por lo que se ha procurado siempre otorgar la máxima seguridad respecto a las características y posibilidades de cada dispositivo

3.6.1 Bluetooth

En la simulación de Bluetooth se ha estudiado como configurar un ASUS N55S, el cual es el equipo que se ha utilizado para hacer el proyecto. En esta simulación se han descrito los siguientes puntos:

- Utilizar autenticación.
- Ocultar Bluetooth y denegar conexión.
- Configurar puertos COM.
- Configurar las propiedades del Hardware.
- Configurar y actualizar los controladores.

3.6.2 Tercera generación/3G

Para la simulación 3G se ha elegido en cambio el dispositivo móvil 3G Samsung Galaxy II, donde al igual que en las anteriores simulaciones se ha configurado este dispositivo de una manera óptima en cuanto a seguridad. Se han realizado las siguientes recomendaciones:

- Desactivar el GPS.
- Agregar VPN.
- Actualizar el dispositivo.
- Establecer contraseñas.
- Descargar e instalar antivirus.
- Paginas https.
- Cifrar contenido.
- Desactivar Wifi.
- Deshabilitar aplicaciones desconocidas.
- Otras aplicaciones y medidas de seguridad.

3.6.3 Wifi

Respecto a las simulaciones llevadas a cabo para la tecnología Wifi se han a cabo dos tipos diferentes de estas: simulaciones de ataques y simulaciones de protección.

En las simulaciones de ataques se ha demostrado como ejecutar y llevar a cabo cada uno de estos ataques, con el fin de que el saber cómo se ejecutan pueda servir para defenderse de ellos de una manera más óptima. Las simulaciones de ataques que se han llevado a cabo son las siguientes:

- Denegación de servicio con Aircrack.
- Denegación de servicio desde Windows.
- Asalto a protocolo WEP con Aircrack.
- Asalto a WEP con Wifiway.
- Asalto a protocolo WPA con Aircrack.
- Asalto a protocolo WPA con Wifislax 4.3.
- Asalto a protocolo WPA/WPA2 con Wifiway.

Por otro lado y al igual que en las tecnologías anteriores también se han llevado a cabo varias simulaciones en cuanto a seguridad. Más concretamente se ha aprendido a:

- Detectar y expulsar intrusos en nuestra red Wifi con ADSL Net.
- Detectar y expulsar intrusos de nuestra red Wifi con NETCUT.
- Como configurar de forma segura un router.

3.6.4 Wimax

Para la tecnología Wimax nuevamente se han llevado a cabo dos simulaciones respecto a medidas de protección, las cuales son las siguientes:

- Restablecer el adaptador de Wimax para Windows.
- Configurar router Wimax.

4 Conclusión final TFC

Como bien se ha visto a lo largo del proyecto, ninguna tecnología o red inalámbrica se puede considerar cien por cien segura, ya sea por las vulnerabilidades que pueda presentar cada una de estas o por el continuo intento por parte de hackers de intentar vulnerar y encontrar cada punto débil de estas.

De todas las redes estudiadas tenemos que resaltar una sobre las demás, en cuanto a seguridad se refiere, es decir la red Wimax. Esta red pese a tener ciertas vulnerabilidades y varios ataques reconocidos contra ella como bien se ha expuesto en el proyecto es prácticamente invulnerable debido principalmente a los certificados X.509 y al potente cifrado que implementa, así como gracias a la propia arquitectura de esta.

La red Wifi por su parte es con diferencia la red más versátil y que permite más opciones en cuanto a configuración de seguridad, pudiendo configurar desde el nombre de nuestra red hasta el tipo de protocolo de red. No obstante y pese a todas las posibles configuraciones que ofrece se podría considerar la red más insegura puesto que es la más vulnerada de todas. El motivo de esto no es que implemente una mala seguridad, ya que incluso puede implementar el protocolo WPA2 y el cifrado AES, cuya combinación es actualmente la más fuerte.

Los motivos de esto son principalmente 3: es muy sencillo captar una señal Wifi; nadie o casi nadie desactiva la señal de emisión Wifi cuando no se está utilizando (esto implica en que un hacker pueda estar todo que desee intentando hackearla); se puede obtener información muy valiosa, pudiendo provocar además mucho daño en caso de que se quiera; y sobre todo hay una masiva cantidad de programas, tutoriales e información a lo largo de internet de como hackear esta red.

Respecto a las redes 3G, bluetooth e infrarrojos, estas también pueden ser igualmente vulneradas, sobre todo la red 3G, ya que es esta la que trabaja con información más sensible.

Por tanto sea cual sea la red que se esté utilizando siempre se deberá seguir el mismo procedimiento de seguridad con el fin de evitar los máximos ataques posibles, es decir configurar plenamente está conforme a todo lo visto en el proyecto y sobre todo utilizarla de una manera debidamente correcta.

Finalmente y para finalizar esta memoria y por consiguiente el proyecto, decir que he disfrutado mucho con la realización de este proyecto, así como también he aprendido muchas cosas muy útiles e interesantes que desconocía de las redes sin hilos.

El motivo inicial que me llevo a elegir esta área fue, entre otros aspectos, la gran utilidad y el provecho que se le podía dar a un tema como este, puesto que todas estas redes, ya sea en mayor o menor medida, juegan un papel vital en las telecomunicaciones y en la sociedad actual, llegando a ser de carácter totalmente indispensable.

Mi objetivo desde un principio fue el de entender por mí mismo en primer lugar que eran cada una de estas redes, cuáles eran sus mecanismos de seguridad y ante que posibles adversidades se podían ver sometidas, para después intentar explicarle al lector de la forma más clara posible todo lo aprendido. Es este objetivo el que perseguí desde el inicio y el que personalmente creo que he cumplido.

5. Bibliografía y glosario

5.1 Bibliografía

- Páginas Web

http://www.ieeespain.org

http://www.ieee.org/publications_standards/index.html

http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica

http://foro.elhacker.net

http://www.arg-wireless.com

http://www.portalhacker.net

http://www.inteco.es/Estudios

http://www.mastermagazine.info

http://www.wimaxforum.com

http://csrc.nist.gov/publications

http://es.wikipedia.org

http://www.hsc.fr

http://timerime.com/es

http://baezjacobotics.blogspot.com.es

http://www.espelectronicdesign.com

http://blog.txipinet.com

http://carlosjaviergonzalezdiaz.blogspot.com.es

http://redesc.wikispaces.com/Seguridad+Wifi

http://www.elprisma.com

http://www.exploit-db.com

- Materiales

Materiales UOC, concretamente de las asignaturas:

- Seguridad en redes de computadores.
- Estructura de redes de computadores.
- Sistemas telemáticos.
- Transmisión digital.
- Redes y servicios.
- Gestión de proyectos.

- Prácticas y Pecs UOC

Prácticas y pruebas de evaluación continua de las asignaturas:

- Seguridad en redes de computadores.
- Sistemas telemáticos.
- Redes y servicios.

- Libros

Seok-Yee Tang, Peter Muller, Hamid Sharif (2010) *Wimax Security and Quality of Service: An End-to-End Perspective.*

José Pico García, David Pérez Conde (2011) *Hacking y Seguridad en Comunicaciones Móviles GSM / GPRS / UMTS / LTE.*

Johnny Cache (2007), *Hacking Exposed Wireless.*

- Estudios y artículos

Karen Scarfone, Cyrus Tibbs, Matthew Sexton. *Guide to Securing Wimax Wireless Communications.*

Matthew Sexton, Cyrus Tibbs, Derrick Dicoi. *Guide to securing legacy IEEE 802.11 Wireless Networks.*

Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone. *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.*

INTECO, *Estudio sobre la seguridad de las redes inalámbricas en los hogares españoles – 1er cuatrimestre de 2012.*

5.2 Glosario

3DES: algoritmo de cifrado que hace triple cifrado del DES.

1G/2G/3G/4G: tecnologías de telefonía de primera, segunda, tercera y cuarta generación.

AAA: comúnmente significa autenticación, autorización y contabilidad. Se refiere a una arquitectura de seguridad para los sistemas distribuidos, que permite controlar qué usuarios pueden acceder a los servicios, y la cantidad de los recursos que han utilizado.

AES: método de encriptación avanzado basado en el algoritmo Rijindael.

AKA: mecanismo de acuerdo/gestión de clave.

AP: punto de acceso a la red.

AUTN: token de autenticación.

AT: comandos usados para dar órdenes de manera directa.

ATM: corresponde al modo de transferencia asíncrono.

AHF: método de frecuencia adaptativa utilizado por la tecnología Bluetooth.

AUC: nodo autenticador el cual forma parte de la arquitectura UMTS.

AD-HOC: una de las diferentes topologías de red existentes.

ARP: protocolo de seguridad utilizado en la capa de enlace.

BS: estación base de una red.

CN: núcleo de red perteneciente a la arquitectura UMTS.

CK: clave de cifrado.

CPE: equipo perteneciente al cliente o usuario final.

CSMA/CA: mecanismo de acceso al medio basado en evitar posibles colisiones.

DoS: ataques de denegación de servicio.

DSSS: técnica de modulación basada en el espectro ensanchado de secuencia directa.

DCHP: protocolo de red que se utiliza para configurar los dispositivos que están conectados a una red.

EDGE: tecnología de telefonía surgido entre la 2.5HG y la 2.75G.

EDR: tecnología utilizada por Bluetooth para aumentar la velocidad de datos.

ESSID: nombre por el que se identifica una red.

EAP: protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, contabilidad y autorización.

GSM: conjunto estándar desarrollado por el Instituto Europeo de Normas de Telecomunicaciones para describir protocolos para redes celulares digitales utilizadas por los teléfonos móviles de segunda generación.

GPRS: tecnología de telefonía surgido entre la 2.5HG y la 2.75G.

GPS: es un sistema de navegación por satélite basado en el espacio que proporciona la ubicación y la hora en todas las condiciones meteorológicas utilizado por la tecnología 3G.

GFSK: versión mejorada de la tecnología de modulación FSK.

HLR: nodo utilizado en las redes de telefonía 3G.

HTTPS: protocolo de comunicaciones utilizado para la comunicación segura a través de una red informática, con especial despliegue en toda la Internet.

HOT-SPOT: punto en el que se ofrece internet a través de Wifi.

IDS: software basado en sistemas de detección antintrusos.

IK: clave de integridad.

IrDA: estándar de codificación utilizado por las comunicaciones de infrarrojos.

IEEE: El Instituto de Ingenieros Eléctricos y Electrónicos es una asociación profesional que se dedica a promover la innovación tecnológica y la excelencia.

IP: corresponde con la dirección IP de un dispositivo.

ICMP: protocolo de control de mensajes usado en internet.

IPSEC: método de encriptación muy robusto.

MAC: dirección física de un dispositivo.

MMS: mensaje multimedia.

MIMC: código de integridad de mensaje.

MITM: ataque man in the middle u hombre en el medio.

MIC: está referida a la abreviatura de Michael.

MIMO: tecnología implantada en Wimax que permite aumentar la velocidad de transmisión.

OFDM: es un método de codificación de datos digitales en múltiples frecuencias portadoras

PSK: tecnología de modulación utilizada por múltiples tecnologías.

QAM: técnica de modulación utilizada por múltiples tecnologías.

RADIUS: protocolo de red que proporciona autenticación centralizada, autorización y gestión de contabilidad.

RNC: controlador de radio de red utilizado en la arquitectura de telefonía.

RSA: algoritmo asimétrico cifrador de bloques que utiliza una clave pública.

RC4: algoritmo de encriptación.

REC80: estándar de codificación utilizado por las comunicaciones de infrarrojos.

RC5: estándar de codificación utilizado por las comunicaciones de infrarrojos.

SS: corresponde con la estación suscriptora de un usuario.

SSH: protocolo de red de cifrado para la comunicación segura de datos, servicios de Shell remotos o ejecución de comandos y otros servicios de red seguras entre equipos.

SAP: etiqueta de identificación para los puntos finales de red utilizados en sistemas abiertos Interconexión en red.

SSID: nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

TCP: protocolo de transporte destacado por la fiabilidad que ofrece.

UMTS: es una de las tecnologías usadas por los móviles de tercera generación, sucesora de GSM, debido a que la tecnología GSM propiamente dicha no podía seguir un camino evolutivo para llegar a brindar servicios considerados de tercera generación.

UE: es el equipo de usuario, el cual es una parte de la arquitectura UMTS.

UTRAN: componente de la red UMTS.

UDP: protocolo de transporte no orientado a seguridad.

VPN: red privada virtual muy útil en cuanto a seguridad.

WPAN/LAN/MAN/WAN: red personal, local, metropolitana y mundial.

WEP/WPA/WPA2: protocolos de seguridad utilizados en redes Wifi.

X.509: certificado de seguridad utilizado por la tecnología Wimax.

6.1 Estándares Wifi

IEEE Standard	Description	Purpose Keywords and Other Remarks	Availability
802.11a	A physical layer standard that operates in the 5 GHz UNII radio band. It specifies eight available radio channels. (In some countries, 12 channels are permitted.) The maximum link rate is 54 Mbps per channel; maximum actual user data throughput is approximately half of that, and the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the AP increases.	**Higher performance** In most office environments, the data throughput will be greater than for IEEE 802.11b. In addition, the greater number of non-overlapping radio channels (eight as opposed to three) provides better protection against possible interference from neighboring APs.	This standard was completed in 1999. Products are available now.
802.11b	This is a physical layer standard in the 2.4 GHz ISM radio band. Maximum link rate is 11 Mbps per channel, but maximum user throughput will be approximately half of this because the throughput is shared by all users of the same radio channel. The data rate decreases as the distance between the user and the AP increases.	**Performance** Installations may suffer from speed restrictions in the future, as the number of active users increase, and the limit of three non-overlapping channels may cause interference from neighboring APs.	This standard was completed in 1999. A wide variety of products has been available since 2001.
802.11d	This standard is supplementary to the MAC layer in IEEE 802.11 to promote worldwide use of IEEE 802.11 WLAN. It will allow APs to communicate information on the permissible radio channels with acceptable power levels for user devices. The IEEE 802.11 standards cannot legally operate in some countries; the purpose of 802.11d is to add features and restrictions to allow WLANs to operate within the rules of these countries.	**Promote worldwide use** In countries where the physical layer radio requirements are different from those in North America, the use of WLANs is lagging behind. Equipment manufacturers do not want to produce a wide variety of country-specific products, and users that travel do not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.	This standard was completed in 2001. Products are available now.
802.11e	This standard is supplementary to the MAC layer to provide QoS support for WLAN applications. It will apply to IEEE 802.11 physical standards a, b, and g. The purpose is to provide classes of service with managed levels of QoS for data, voice, and video applications.	**Quality of service** This standard provides some useful features for differentiating data traffic streams. It is essential for future audio and video distribution.	This standard was completed in 2005. Products are available now.

802.11f	This is a "recommended practice" document that aims to achieve AP interoperability within a multi-vendor WLAN. The standard defines the registration of APs within a network and the interchange of information between APs when a user is handed over from one AP to another.	**Interoperability** This standard will work to increase vendor interoperability, reduce vendor lock-in, and allow multi-vendor infrastructures.	This recommended practice was completed in 2003. Products are available now.
802.11g	This is a physical layer standard for WLANs in the 2.4 GHz ISM radio band. The maximum link rate is 54 Mbps per channel whereas IEEE 802.11b offers 11 Mbps. The IEEE 802.11g standard uses orthogonal frequency-division multiplexing (OFDM) modulation but, for backward compatibility with IEEE 802.11b, it also supports complementary code-keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolutional coding (PBCC) modulation.	**Higher performance with IEEE 802.11b backward compatibility** This standard provides speeds similar to IEEE 802.11a and backward compatibility with IEEE 802.11b.	This standard was completed in 2003. Products are available now.
802.11h	This standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the farthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.	**European regulation compliance** This is necessary for products to operate in Europe. Completion of IEEE 802.11h provides better acceptability within Europe for IEEE-compliant 5 GHz WLAN products. A group that is rapidly dwindling will continue to support the alternative HyperLAN standard defined by the European Telecommunications Standard Institute (ETSI).	This standard was completed in 2003. Products are available now.
802.11i	This standard is supplementary to the MAC layer to improve security. It applies to IEEE 802.11 physical standards a, b, and g. It provides improved security over Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1X forms a key part of IEEE 802.11i.	**Improved security** The IEEE 802.11i amendment defines two data confidentiality and integrity protocols for Robust Security Network Associations (RSNA): TKIP and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), using AES. Federal agencies are required to use FIPS-validated cryptographic modules.[32] NIST SP 800-97 contains specific recommendations and guidance for IEEE 802.11i.	This standard was completed in 2004. Products are available now.

802.11k	This standard defines Radio Resource Measurement enhancements to provide management and maintenance interfaces to higher layers for mobile WLANs.	**Resource radio management** This standard will enable seamless Basic Service Set (BSS) transitions between WLANs through the discovery of the best available AP and improve network traffic by distributing users to under-used APs.	Draft 11 was approved in January 2008. Final ratification has not yet occurred.
802.11m	This is a supplementary maintenance standard to the IEEE 802.11-1999 (reaff. 2003) standard.	**Editorial maintenance** This initiative is to perform editorial maintenance, corrections, improvements, clarifications, and interpretations to the IEEE 802.11-1999 (reaff. 2003) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications standard.	This standard was completed and is part of 802.11-2007.
802.11n	This standard investigated the possibility of improving the IEEE 802.11 standard to provide high throughput at a theoretical 300 Mbps.	**Increased data throughput** The purpose of this standard is to improve the IEEE 802.11 WLAN user experience by providing significantly higher throughput using MIMO antennas and receivers and different coding schemes.	This standard is expected to be completed in 2009.
802.11p	This standard is an amendment of IEEE 802.11 to support communication between vehicles and the roadside and between vehicles while operating at speeds up to a minimum of 200 kilometers/hour for communication ranges up to 1,000 meters. The amendment will support communications in the 5 GHz bands—specifically 5.850–5.925 GHz band within North America—with the aim to enhance the mobility and safety of all forms of surface transportation, including rail and marine.	**Wireless access for vehicles** This standard amends the existing IEEE 802.11 standard to make it suitable for interoperable communications to and between vehicles. The primary reasons for this amendment include the unique transport environments and the very short latencies required (some applications must complete multiple data exchanges within 4 to 50 milliseconds).	This standard is scheduled to be completed in April 2009.

802.11v	This standard will create amendments to provide Wireless Network Management enhancements to the IEEE 802.11 MAC, and PHY layers to allow configuration of client devices connected to the network.	**Wireless network management** This will provide amendments to the IEEE 802.11 PHY/MAC layers that enable management of attached stations in a centralized or in a distributed fashion (e.g., monitoring, configuring, and updating) through a layer 2 mechanism. Although the IEEE 802.11k Task Group is defining messages to retrieve information from the station, the ability to configure the station is not within its scope. The proposed Task Group will also create an Access Port Management Information Base (AP MIB).	This standard is in the early proposal stages and a scheduled completion date has not been set.
802.11w	This standard will enhance IEEE 802.11 MAC layer security for selected management frames by providing data integrity, data origin authenticity, replay protection, data confidentiality, and other security features.	**Management frame protection** This will extend the use of IEEE 802.11i to selected management frames to increase the overall security of IEEE 802.11-based networks. The increased level of security is intended to mitigate malicious network-based attacks, such as DoS attacks. In addition, this amendment will provide security for sensitive network information that will be included in transmissions outlined in several new amendments, including IEEE 802.11r, IEEE 802.11k, and IEEE 802.11y.	The standard is under development and is expected to be completed and ratified in 2008.

802.11r	This standard is supplementary to the IEEE 802.11 Medium Access Control (MAC) layer standards and creates improvements to minimize or eliminate the amount of time data connectivity between the Station (STA) and the Distribution System (DS) during a BSS transition.	**Fast BSS transitions** This standard improves BSS handoffs within IEEE 802.11 networks. This is a critical component to support real-time constraints imposed by applications such as Voice over Internet Protocol (VoIP).	This standard is scheduled to be published in mid-2008.
802.11s	This standard defined the IEEE 802.11 ESS Mesh with an IEEE 802.11 Wireless Distribution System (WDS) using the IEEE 802.11 MAC/PHY layers that supports both broadcast/multicast and unicast delivery over self-configuring multi-hop topologies.	**ESS mesh networking** This standard provides a protocol for auto-configuring paths between APs over self-configuring multi-hop topologies in a WDS to support both broadcast/multicast and unicast traffic in an ESS Mesh using the four-address frame format or an extension.	This standard is scheduled to be completed in 2008.
802.11t	This is a "recommended practice" and will provide a set of performance metrics, measurement methodologies, and test conditions to enable measuring and predicting the performance of IEEE 802.11 WLAN devices and networks at the component and application level as a recommended practice.	**Wireless performance protection** This standard enables testing, comparison, and deployment planning of IEEE 802.11 WLAN products so that performance and products specifications can be captured through common and accepted set of performance metrics, measurement methodologies and test conditions.	This recommended practice is scheduled to be completed in 2008.
802.11u	This standard is an amendment to the IEEE 802.11 MAC and PHY layers to support InterWorking with External Networks.	**Internetworking with external networks** This will provide amendments to the IEEE 802.11 PHY/MAC layers, which will enable InterWorking with other networks and granting of limited access, based on a relationship with an external network. This includes both enhanced protocol exchanges across the air interface and provision of primitives to support required interactions with higher layers for InterWorking.	This standard is in the proposal evaluation stages and a scheduled completion date has not been set.

6.2WLNA Best practices

Table 8-1. IEEE 802.11 RSN Security Checklist: Initiation Phase

Initiation Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
1	Perform a risk assessment to understand WLAN threats, the likelihood that those threats will be realized, and the potential impact of realized threats on the value of the organization's assets.[99]	The risk assessment is an important input to the development of the WLAN usage policy because it identifies which WLAN activities pose an acceptable risk to the organization's information resources and which do not.	ALL	✓		
2	Establish a WLAN usage policy that specifies which user communities are authorized to use WLAN technology and for what purposes.	A WLAN usage policy is the foundation on which subsequent security controls are based. It should be defined and enforced by WLAN trained staff or consultants. The policy should explicitly identify if WLANs are available to business partners, customers, and other guests. It should also identify the information resources that shall and shall not be available to WLAN users (e.g., allow a guest to use the organization's Internet connection but not access its internal database servers). Finally, the policy should describe the terms under which an organization's WLAN-capable mobile devices (e.g., laptops) can be used on external WLANs (e.g., home, hotel, coffee shop).	STA / AP/AS	✓		
3	Require that all connections to an organization's WLANs be based on an IEEE 802.11i RSNA using IEEE 802.1X/EAP authentication.	Sections 3 and 4 detail the reasons why RSN associations are superior to pre-RSN authentication techniques. The RSNAs should be based on IEEE 802.1X/EAP authentication rather than pre-shared keys. Also, the RSNAs should use CCMP leveraging a FIPS-validated AES encryption module. Organizations may relax this requirement for public-use WLANs if they disclose that those WLANs provide no security for wireless connections; if so, they may require a captive portal ("splash page") system to provide users with relevant legal disclosures and disclaimers.	STA	✓		

Initiation Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
4	Establish or enhance operating system and application security configuration standards for laptops and other potential STAs to account for WLAN risks.[100]	WLAN-capable devices typically are at greater risk of a security breach than wired-only devices and may require additional security controls beyond those already present. The configuration standard should require personal firewall and anti-virus software for all STA platforms for which such security products are commercially available. Remote connectivity to the devices (e.g., file sharing, open network ports) should be limited where feasible.	STA	✓		
5	Establish or enhance operating system and application security configuration standards for the AS.	The ASs should be among the most secure servers in the enterprise because a breach of an AS could allow an adversary to access the network without a physical connection, perhaps even beyond the organization's physical perimeter. Special emphasis should be placed on preventing exposure of cryptographic keys to unauthorized parties.	AS	✓		
6	Require that administration and network management of WLAN infrastructure equipment (i.e., APs and ASs) involve strong authentication and encryption of all communication.	IEEE 802.11i does not specify any requirements related to the management and administrative interfaces of WLAN equipment, so it cannot be assumed that these interfaces are secure. If an organization uses Simple Network Management Protocol (SNMP) to manage its equipment, it should use SNMPv3,[101] which has enhanced security features relative to its predecessors. Web-based administration should use SSL/TLS or an equivalent protection (e.g., IPsec).[102] Secure shell (ssh) and secure ftp (sftp) can be used for command-line access and file uploads.	AP / AS	✓		

Initiation Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
7	Educate users about the risks of WLAN technology and how to mitigate those risks.	Security awareness and training helps users to establish good security practices to prevent inadvertent or malicious intrusions into an organization's information systems. WLAN security content should be integrated into existing security awareness programs when feasible.[80]	ALL	✓		
8	If applicable, develop or revise the organization's PKI certificate policy, certification practice statement, and related processes to support the WLAN solution.	The certificate policy and certification practice statement are the foundation of PKI security. An IEEE 802.11i RSN can leverage a PKI if it uses IEEE 802.1X port-based access control with an EAP method based on public key cryptography, which is expected to be the case in nearly all large enterprises that deploy RSNs. A PKI may also be used to support IPsec connections that supplement the RSN solution (e.g., for securing communication between AP and AS, which is not required in WLAN standards). This recommendation is not applicable in environments without a PKI and may not be applicable in environments that use the PKI services of a third party.[181]	STA / AS	✓		
9	Require two-factor authentication for WLAN connectivity.[182]	Two-factor authentication enhances the strength of the authentication procedure, making it less likely that adversaries will successfully exploit it. Two-factor authentication could include use of biometrics or smart cards, which could significantly increase the cost of the WLAN solution. Organizations should weigh the costs and benefits of any proposed authentication solution. For users, devices whose credentials cannot be re-used require re-authentication when roaming from one AP to another; this makes this approach cumbersome and potentially unusable. In cases in which two-factor authentication is determined to be unnecessary for users, it should still be considered for administrative connections to WLAN infrastructure.	STA / AS		✓	

Initiation Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
10	Establish requirements for a WLAN intrusion detection system.[186]	Intrusion detection systems deployed on the wireless network can detect and respond to potential malicious activities, including unauthorized WLAN vulnerability scanning and the installation of rogue APs. The results of the risk assessment should help determine the level (if any) of intrusion detection required.	STA / AP / DS	✓		
11	Use the services of security professionals to assist with WLAN security issues if the requisite skill sets are not currently available in the organization.	Wireless security is a complex field. Even small flaws in implementation can have significant ramifications for the resulting security of the WLAN solution. Well-trained professionals can help mitigate this risk.	ALL		✓	

Planning and Design Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
12	Conduct a site survey to determine the proper location of APs, given a desired coverage area.	The site survey should result in a report that proposes the location for each AP, graphically notes its usable coverage area, and assigns it an IEEE 802.11 radio channel.[187] The estimated usable range of each AP should not extend beyond the physical boundaries of the facility whenever possible. To best achieve this result, APs should be located near the center of rooms and away from exterior walls and windows. In addition, APs should be located in areas that can be physically secured to prevent unauthorized tampering.[188] Configuring APs to only accept connections at higher data rates helps limit the effective coverage area as well.	AP		✓	
13	Create a dedicated Virtual LAN (VLAN)[189] to support AP connections to the distribution system (e.g., enterprise wired network).	Using dedicated VLANs to support wireless connections to the enterprise network segregates wireless traffic from other network communications. Dedicated VLANs facilitate the use of network access control lists, which identify the protocols and services that are allowed to pass from WLANs to the DS. Different VLANs can be defined within the wireless connections to further separate varying security policies.	AP / DS		✓	

Planning and Design Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
14	Ensure that network management information between APs/ASs and network management servers or consoles is transmitted over a dedicated management VLAN.	This control is applicable only in cases in which APs or ASs can support a dedicated management interface. A dedicated management VLAN can be used to transfer pre-shared keys, execute management commands, and transmit audit data without the risk that non-administrative users can eavesdrop on that communication. Segregating this type of traffic is often referred as out of band communication because it occurs over a separate channel than those that support data traffic. Out of band channels are particularly useful during denial of service attacks, when severe congestion on data channels may prevent administrators from implementing corrective security measures if those data channels are the only ones available to them. This sensitive VLAN traffic should be protected.	AP / AS		✓	
15	If a WLAN will be supporting unauthenticated users, such as members of the public, install a network firewall between each WLAN and its distribution system.[119]	A firewall can enforce a security policy on the information flow between the WLAN and its distribution network, allowing only authorized protocols and services to traverse this boundary. Firewalls are necessary if access to the WLAN is extended to users who are not positively identified by 802.11i, such as members of the general public.	AP / AS / DS		✓	
16	Install a personal firewall on each mobile device.	A personal firewall can enforce a security policy on the information flow between the STA and other parties, allowing only authorized protocols and services to access the STA. This can prevent direct attacks on the STA before the completion of the 4-Way Handshake; it can also prevent attacks from other clients attached to the same AP after the completion of the 4-Way Handshake.	STA	✓		

Planning and Design Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
17	Develop wireless security audit processes and procedures that identify the types of security relevant events that should be captured, and determine how audit records will be securely stored for subsequent analysis.	Developing a program of audit processes and procedures will help ensure that the organization can detect unauthorized behavior and security breaches on wireless systems. Both APs and ASs should send event data to a secure audit server in real time so that the integrity of previously captured audit data is protected even when the AP or AS is compromised. Events to be captured should include, at a minimum, both successful and unsuccessful authentication and association attempts.	AP / AS	✓		
18	Select an appropriate EAP method or EAP method sequence for WLAN authentication, and design any necessary integration with PKI technology.	EAP method selection is the cornerstone of RSN security protections; a poor EAP implementation can undermine nearly all aspects of RSN security. Appropriate EAP methods are those that meet the required security claims listed in Section 5.1.2. They usually will include one or more of the TLS-based methods (e.g., EAP-TLS, EAP-TTLS, PEAP) because TLS is the preferred method for distributing key material. If the TLS method uses an inner application or method, these should also be identified at this time. All TLS methods require at least some integration with a PKI, even if certificates are required on ASs only. Careful planning of the authentication methods and supporting infrastructure ensures that RSNAs will comply with the organization's security policy and objectives.	STA / AS	✓		
19	Determine the fallback strategy when WLAN authentication fails.	Authorized users sometimes fail to successfully authenticate to the WLAN, even though they have a valid business reason to use the network. Reasons include forgotten passwords and lost smart cards. There should be a fallback strategy to provide access to these users. In some cases, this might involve a human process such as a call to the help desk to reset a password. In other cases, it might involve a technical process, such as providing users the ability to enter a pass phrase when they are using a STA that does not hold a personal certificate. In either situation, the fallback method should be at least as strong as the primary method, otherwise attackers will attempt to exploit the weaker fallback approach.	AS	✓		

Planning and Design Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
20	Deploy wireless intrusion detection systems to detect suspicious or unauthorized activity.	Intrusion detection systems enable the organization's operations or security staff to identify and respond to attacks on the organization's systems or information resources before they inflict the maximum potential damage. The radio coverage of wireless intrusion detection devices should be at least as great as that of the WLANs they are intended to protect. If the coverage area of the intrusion detection system were smaller than the coverage area of the WLAN, then attackers could position themselves to circumvent the intrusion detection system.	STA / AP	✓		

Table 8-3. IEEE 802.11 RSN Security Checklist: Procurement Phase

Procurement Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
21	Procure WPA2-Enterprise certified STA and AP products only. [11]	Only WPA2-Enterprise certified products are capable of fully implementing the IEEE 802.11i RSN protections, including CCMP support and IEEE 802.1X port-based access control.	STA / AP	✓		
22	Procure products that use FIPS-validated cryptographic modules and deploy them in "FIPS mode" if required. [12]	Federal agencies are required to use FIPS-validated cryptographic modules. Cryptographic modules that are not FIPS-validated cannot be assured of providing the level of cryptographic protection intended through use of RSN technology. When reviewing the list of a vendor's FIPS-validated products, organizations should check that the validation is for the algorithms that will be deployed in the organization's RSN (e.g., CCMP).	STA / AP	✓		

Procurement Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
23	Procure STAs and APs that support NIST AES key wrap with 128-bit HMAC-SHA-1 to protect transient keys during the 4-Way and Group Key Handshakes.	AES provides assurance of key confidentiality, while HMAC-SHA-1 provides assurance of key integrity. Protecting the PTK and GTK during transit is critical to protecting the communications that rely on those keys for data confidentiality and integrity. The alternative algorithm permitted by IEEE 802.11i for the 4-Way and Group Key Handshakes is RC4 encryption (for confidentiality) with HMAC-MD5 (for integrity), but RC4 has known vulnerabilities, and neither algorithm is FIPS-validated.	STA / AP	✓		
24	Procure ASs and APs that communicate in a secure manner.	The communication link between the AS and AP should be secured. The MSK distribution from AS to AP should use appropriate key wrap mechanisms.	AS/AP	✓		
25	Procure products that support the organization's chosen EAP methods.	If the organization invests in products that do not support the chosen EAP methods, then either the equipment cannot be used (resulting in wasted expenditure) or pressure may exist to modify the organization's security configuration to support alternative methods, which might weaken the network security. Both STAs and ASs must support the chosen EAP methods. Organizations should test EAP interoperability between STAs and ASs before final procurement.	STA / AS	✓		
26	Procure APs that terminate associations after a configurable time period.	IEEE 802.11i does not specify the length of time for which an RSN association is valid, potentially allowing WLAN sessions to remain open indefinitely. A session termination feature in the AP would cause STAs to reauthenticate if network access is still needed after a fixed period of idleness or connectivity. While not required by the standard, this functionality mitigates the risk that an adversary could use active RSN associations for unauthorized purposes for an indefinite period of time.	AP	✓		

Procurement Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
27	Procure ASs that grant authorizations for a configurable time period.	IEEE 802.11i does not specify the length of time for which an RSN association is valid, potentially allowing WLAN sessions to remain open indefinitely. A session termination feature in the AS would cause STAs to reauthenticate if network access is still needed after a fixed period of idleness or connectivity. While not required by the standard, this functionality mitigates the risk that an adversary could use active RSN associations for unauthorized purposes for an indefinite period of time.	AS		✓	
28	Procure APs that log security relevant events and forward them to a remote audit server in real time[113].	Audit technology helps ensure that the organization can detect unauthorized behavior and take actions to prevent or limit the extent of a security breach. IEEE 802.11i does not require a logging capability, so organizations must seek this functionality outside the standards framework. The AP should support the functional audit requirements developed during the planning and design phase. The AP should have a feature to forward events automatically to a central audit server.	AP	✓		
29	Procure APs that can support an independent management interface to the distribution system (e.g., wired network).	Support for an independent management interface enables organizations to establish an out of band channel for key transfer and other administrative functions.	AP		✓	
30	Procure APs that support SNMPv3 if the organization plans SNMP-based AP management.	SNMPv3 has enhanced security features relative to its predecessors.	AP		✓	
31	Procure APs that support authentication and data encryption for administrative sessions.	IEEE 802.11i does not specify security for administrative connections to APs, potentially allowing unauthorized management of these devices if not properly secured. Examples of protections include SSL/TLS support for Web-based administration and secure shell (SSH) for command-line administration.	AP	✓		

Procurement Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
32	When the WLAN solution involves TLS-based EAP methods, procure STAs whose software can be configured to specify valid ASs by name.	If a STA does not specify the valid servers with which it can authenticate, a potential exists for an adversary to insert a bogus AS into the WLAN infrastructure as part of a man-in-the-middle attack.	STA	✓		
33	Procure APs and ASs that can support IPsec or alternative security methods to establish a mutually authenticated secure communications channel between AP and AS.[114]	IEEE 802.11i and its related standards (IEEE 802.1X, EAP, etc.) assume a preexisting trust relationship between the AP and AS and further assume that the communication between them is secure. If organizations do not implement technology to realize these characteristics, then the assumptions are invalid and RSN security could be compromised. IPsec is the most common means of establishing a secure communications channel between two devices, but equivalent protection can be provided with link layer security controls and other protocols designed to ensure the confidentiality and integrity of network communications.[115]	AP / AS	✓		
34	Procure APs and ASs that support Network Time Protocol (NTP).	NTP allows distributed devices to synchronize timestamps, which is critical to effective log analysis because it allows audit personnel to establish accurate event sequences across multiple devices. In addition, IEEE 802.11i suggests that the nonce in the 4-Way Handshake should be based on NTP time whenever possible. If not, the cryptographic properties of the 4-Way Handshake could be weakened in some circumstances.	AP / AS		✓	
35	Procure an auditing tool to automate the review of AP and AS audit data.	Audit tools often are more effective than humans at distilling relevant information from multiple sources. In large enterprise WLAN deployments, reviewing the amount of data generated could overwhelm technical support staff if they do not have appropriate tools to assist them with this task.	AP / AS / DS	✓		

Procurement Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
36	Procure products that can be upgraded easily in software or firmware.	WLAN products require this support so that they can take advantage of wireless security patches and enhancements released after original delivery. Not all APs support this feature, so this functionality should be verified before procurement.	ALL	✓		

Table 8-4. IEEE 802.11 RSN Security Checklist: Implementation Phase

Implementation Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
37	Ensure that all APs have strong, unique administrative passwords.	To protect against dictionary attacks, administrator passwords on APs should be hard to guess. In addition, organizations should not use a common password for multiple APs. Otherwise, a compromised password on one AP could have much wider consequences.	AP	✓		
38	Disable all insecure and unused management protocols on the APs, and configure remaining management protocols for least privilege.	Disabling all insecure and nonessential management protocols eliminates potential methods that an adversary can use when attempting to compromise an AP. Examples of insecure management protocols include SNMPv1 and SNMPv2. If SNMPv3 is used, configure it for least privilege (i.e., read only) unless write access is required (e.g., to change configuration settings as part of an automated incident response procedure).	AP	✓		
39	Disable WEP and TKIP in the configuration of each AP.	If WEP remains enabled, then STAs might be able to negotiate WEP for authentication and encapsulation, which would negate RSN protections. Similarly, if an organization's security policy requires CCMP, but TKIP remains enabled, then STAs might negotiate TKIP instead of CCMP. [116]	AP	✓		

Implementation Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
40	Activate logging and direct log entries to a remote audit server.	Logs enable security and support staff to identify potential security issues and respond accordingly. Using a remote central logging server facilitates reviews of logs across the enterprise and ensures the integrity of log data when the AP or AS is compromised.	AP / AS	✓		
41	Establish an IPsec connection (or equivalent protection mechanism) between each AP and its associated AS or ASs.	The standards assume that the AP and AS have a preexisting trust relationship but never specify how that relationship is established. A mutual authenticated secure connection between AP and AS must exist to prevent an adversary with access to the distribution system from impersonating the AS or eavesdropping on the transfer of key material among other potential attacks. Exploits of this nature could greatly undermine the efficacy of RSN protections.	AP / AS		✓	
42	Configure a maximum GMK lifetime on the AP, preferably not to exceed 24 hours.	The GMK is used to protect multicast traffic. Setting a maximum GMK lifetime reduces the exposure of data if the GMK is ever compromised.	AP	✓		
43	Configure a maximum PMK lifetime on the AS, preferably not to exceed eight hours. [117]	In the IEEE 802.11i RSN framework, the PMK is used to derive all other encryption keys used to secure various types of WLAN communication. Setting a maximum lifetime for the PMK reduces the probability that an adversary can compromise it.	AS	✓		
44	Configure the STA and AS to use authorized EAP methods only.	If both the STA and AS allow EAP methods other than those permitted in the security architecture, then a potential exists that the STA and AS will use the unauthorized method in a manner that circumvents the organization's security policy.	STA / AS	✓		
45	When TLS methods are used, ensure that the STAs connect to valid ASs only.	If a STA connects to an unauthorized AS, that AS will be able to capture authentication credentials and severely compromise network security. To ensure authorized connections, the STA should be configured to specify the names of valid ASs, specify the locally stored CA certificate used to validate the digital signature of the AS certificate, and require that the STA check for AS certificate revocation.	STA	✓		

Implementation Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
46	Disable ad hoc mode on each STA unless a business requirement exists for peer-to-peer wireless networking.	Most organizations that deploy WLANs use infrastructure mode only, in which STAs connect to an enterprise network through APs. Attackers can use ad hoc mode to gain access to a computer's information resources with little effort, particularly when the STA is configured improperly (e.g., default settings have not been changed). The wireless IDS should monitor the use of ad hoc mode on the wireless network. Organizations that require ad hoc mode should develop and apply a standard configuration to each STA and develop procedures for implementing and replacing pre-shared keys.	STA	✓		

Table 8-5. IEEE 802.11 RSN Security Checklist: Operations/Maintenance Phase

Operations/Maintenance Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
47	Test and deploy software patches and upgrades on a regular basis.[118]	Newly discovered security vulnerabilities of vendor products should be patched to prevent inadvertent and malicious exploits. Patches should also be tested before implementation to ensure that they work properly.	ALL	✓		
48	Ensure that all passwords are changed regularly.	Passwords should be changed regularly to reduce the risk of a compromised password being misused; it may be possible to configure the user management system to enforce password updates.	ALL	✓		
49	Review audit logs frequently.	Frequent reviews of audit logs allow security and support personnel to identify security issues and take corrective or preventative measures quickly. All components of the WLAN solution should generate event logs, especially the AP and AS. Automated logging tools can assist with log review and send real-time alerts in response to critical events. Events to track include failed authentication attempts and MIC failures.	AP / AS / DS (STA optional)	✓		

Operations/Maintenance Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
50	Inventory APs.	A complete inventory of an organization's authorized APs is the basis for identifying rogue APs during security audits and can be helpful for a variety of support tasks.	AP	✓		
51	Inventory STAs.	STAs have the potential to provide an adversary with an entry point into the enterprise network, particularly if a user has activated ad hoc mode, which allows peer-to-peer connections from other STAs. Understanding where STAs are located and how they are used can assist with risk assessments, audits, and other support tasks. Taking an inventory of STAs is most practical in organizations that already have mature asset management systems.	STA	✓		
52	Perform comprehensive WLAN security assessments at regular and random intervals.	Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and identifying corrective actions necessary to maintain acceptable levels of security. WLAN security assessments should include radio detection of rogue APs; verification of STA, AP and AS configuration settings; and review of audit logs.	AP / AS	✓		
53	Re-apply the organization's security configuration standard to an AP whenever its reset function is used.	Security settings typically are returned to factory defaults after a reset event, which usually occurs when an AP experiences an operational failure. Appropriate personnel need to restore the standard security configuration to ensure that RSN protections are maintained whenever a reset occurs.	AP	✓		
54	If an organization uses PSKs to establish RSN associations, replace them frequently, preferably at least every 30 days.	Most organizations do not require PSKs, relying instead on the alternative key management techniques integrated with various EAP methods. Organizations that distribute pre-shared keys, either manually or through proprietary automated solutions, need to replace the keys periodically to reduce the risk that they will be compromised.[119]	STA / AP	✓		
55	If PSKs are used to establish RSN associations, ensure that no key is shared across multiple STAs.	Ensuring the uniqueness of each PSK limits the impact of a key compromise on communications between the STA and AP that hold the key. If any STA/AP combination shares a PSK with another STA/AP combination, a STA or AP in one pair could compromise the communication of the other pair.	STA / AP		✓	

Operations/Maintenance Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
56	Periodically update the certificates on the clients and the servers.	This is especially important on client devices, which must have accurate root and intermediate CA certificates loaded locally in order to be able to authenticate the AS correctly.	STA / AP		✓	
57	Designate an individual or group to track WLAN product vulnerabilities and wireless security trends.	Assigning responsibility to an individual for tracking wireless security issues helps ensure continued secure implementation of the organization's WLANs.	ALL	✓		

Table 8-6. IEEE 802.11 RSN Security Checklist: Disposition Phase

Disposition Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
57	When disposing of a WLAN component, remove all sensitive configuration information, including pre-shared keys and passwords.	Adversaries can use sensitive information on discarded devices to conduct subsequent attacks on the organization's networks. Organizations should use degauss devices when feasible.[120] Disk wiping utilities can be used for devices that have hard disks. Another option is to clear configuration settings manually using the management interface.	ALL	✓		

Disposition Phase						
#	Security Recommendation	Rationale / Discussion	Impacted Components	Checklist		
				Best Practice	Should Consider	Status
58	When disposing of a WLAN component, ensure that its audit records are retained as needed to meet legal or other requirements.	Information contained in the audit records may be needed even after the WLAN component is discarded (e.g., for an investigation of a subsequently discovered security breach). Organizations should identify the legal requirements to retain records that apply to their operations.[121] When log events are forwarded to a central audit server, as is recommended, regular backup of the server facilitates the retention of records. When a log server does not exist, the disposal process needs to include capturing the existing log data and storing it on alternative media, such as CD-ROM or tape.	ALL	✓		

6.3 Security Wimax

Security Concern or Vulnerability	Threat Discussion	Countermeasure
IEEE 802.16-2004 Based WiMAX Systems		
Unilateral authentication of SS by BS	SSs have no method for verifying the identity of BSs. This leaves SSs susceptible to forgery attacks by a rogue BS. This may result in degraded performance, information theft, or DoS attacks. In addition, this authentication schema leaves a system susceptible to man-in-the-middle attacks.	Force communications to take place over a VPN or encryption overlay that authenticates the devices/users outside of the WiMAX system's native controls.
DES-CBC Weakness	DES-CBC is a weak algorithm that cannot ensure confidentiality of data. Using DES-CBC may lead to unauthorized disclosure of information. Threats may include DoS, eavesdropping, and man-in-the-middle attacks.	Implement an encryption overlay or VPN that employs a FIPS-validated solution, i.e., FIPS-validated encryption algorithms and FIPS-validated cryptographic modules
Interjection of Reused TEK	The short two-bit TEK identifier wraps to zero on every fourth re-key. This allows adversaries to reuse expired TEKs and perform replay attacks leading to unauthorized disclosure of information and compromise of the TEK.	Implement encryption overlay or VPN that employs a FIPS-validated solution, i.e., FIPS-validated encryption algorithms and FIPS-validated cryptographic modules
All WiMAX Systems		
Unencrypted Management Messages	BSs and SSs/MSs communicate using unencrypted management messages to facilitate network entry, node registration, bandwidth allocation, and ranging. These messages are not encrypted. Integrity checks are added to unicast messages to prevent replay attacks; however, non-unicast messages are still vulnerable to DoS attacks. Unencrypted management messages are subject to eavesdropping, replay attacks, scrambling, and subtle manipulation aimed at degrading service. If a system is not using AES-CCM, it remains vulnerable to a man-in-the-middle attack.	There is no threat mitigation for unencrypted management messages; however, AES-CCM helps to mitigate against man-in-the-middle attacks. The impact from management message exploitation is exposure of node registration information and various DoS attacks. It is recommended that organizations plan for out-of-band communications in the event of a DoS attack. At a minimum, organizational SOPs should include DoS incident response plans.
Lack of Native FIPS-Validated Solutions	As of mid-2010, most WiMAX vendors had not completed the FIPS-validation process. This prevents Federal entities from relying on native WiMAX security until vendors complete the validation process. Communications relying solely on unvalidated native WiMAX security to protect confidentiality may be vulnerable to encryption implementation weaknesses that may lead to unauthorized disclosure of information. These threats include eavesdropping, man-in-the-middle, and DoS attacks.	Implement encryption overlay or VPN that employs a FIPS-validated solution, i.e., FIPS-validated encryption algorithms and FIPS-validated cryptographic modules.
Use of Wireless as a Communications Medium	DoS attacks can be executed by the introduction of a powerful RF source intended to overwhelm system radio spectrum.	Locate and remove the source of RF interference. This can be challenging because of the large coverage areas of WMANs. It is recommended that organizations plan for out-of-band communications in the event of a DoS attack.