

Ataques a las comunicaciones sin hilos y sus principales métodos de mitigación

Memoria Final

Laura Rasal Blasco



Contenido

1. Introducción	6
2. Introducción a las redes sin hilos	7
2.1 Tipos de redes sin Hilos	7
2.2 Introducción al funcionamiento del estándar 802.11	10
2.2.1 Definición del estándar 802.11	10
2.2.2 Principales usos del estándar 802.11	12
2.2.3 Descripción del funcionamiento de 802.11	12
2.2.4 Medidas de seguridad 802.11	13
2.3 Introducción al funcionamiento del estándar Bluetooth	18
2.3.1 Definición del estándar Bluetooth	18
2.3.2 Principales usos del estándar Bluetooth	19
2.3.3 Descripción del funcionamiento de Bluetooth.	20
2.3.4 Medidas de seguridad Bluetooth	21
2.4 Introducción al funcionamiento del RFID	23
2.4.1 Definición del estándar RFID	23
2.4.2 Principales usos del estándar RFID	24
2.4.3 Introducción al funcionamiento RFID	24
2.4.4 Medidas de seguridad RFID	25
2.5 Introducción al funcionamiento del NFC	26
2.5.1 Definición del estándar NFC	26
2.5.2 Principales usos del estándar NFC	26
2.5.3 Introducción al funcionamiento NFC	27
2.5.4 Medidas de seguridad NFC	30
3. Seguridad de la información	32
3.1 Concepto de Seguridad de la Información	32
3.1.1 Confidencialidad	32
3.1.2 Integridad	33
3.1.3 Disponibilidad	35
3.2 Clasificación de los ataques en base al proceder de los atacantes	36
3.2.1 Ataques pasivos	36
3.2.2 Ataques activos	36
3.2.3 Ataques de autenticación	37
4. Riesgos, Amenazas y Vulnerabilidades en Redes Sin Hilos	37
4.1 Ataques sobre la pérdida de confidencialidad	37
4.1.1 Interceptación o Sniffing / Eavesdropping	38

4.1.2	Ataques “Man in the Middle” o de intermediario.....	39
4.2	Ataques sobre la pérdida de Integridad	40
4.2.1	Corrupción de datos	40
4.2.2	Modificación de datos.	41
4.3	Pérdida de Disponibilidad	41
4.3.1	Denegación de servicio.....	41
4.4	Resumen	42
5.	Ataques específicos a tecnologías sin hilos.....	42
5.1	Ataques a la tecnología 802.11	42
5.1.1	Ataques para acceso al medio.....	42
5.1.2	Falsificación de identidad.....	46
5.1.3	Rogue Access Points	46
5.1.4	El robo de información vía redes Wi-Fi (Wi-phishing)	47
5.1.5	MAC Address Spoofing	48
5.1.6	Vulnerabilidad Hole 196.....	48
5.2	Ataques a la tecnología Bluetooth.....	49
5.2.1	Ataques a implementación de Bluetooth en terminales móviles.....	49
5.2.2	Ataques a implementación de Bluetooth en manos libres.....	57
5.3	Ataques a la tecnología RFID	60
5.3.1	Ataque a los elementos tecnológicos del RFID	60
5.4	Ataques a la tecnología NFC	61
5.4.1	Redirección a sitios maliciosos a través de las etiquetas NFC.....	61
6.	Mitigación de los riesgos y ataques a las comunicaciones inalámbricas.....	61
6.1	Mitigación de los riesgos y ataques en el estándar 802.11.	62
6.1.1	Valoración personal a cerca de los mejores métodos para mitigar los riesgos del protocolo 802.11.....	62
6.1.2	Posibles aspectos a mejorar del estándar 802.11.....	63
6.2	Mitigación de los riesgos y ataques en el protocolo Bluetooth.....	64
6.2.1	Valoración personal a cerca de los mejores métodos para mitigar los riesgos del protocolo Bluetooth.....	65
6.2.2	Posibles aspectos a mejorar en el estándar Bluetooth.	65
6.3	Mitigación de los riesgos y ataques en el protocolo RFID.....	66
6.3.1	Valoración personal a cerca de los mejores métodos para mitigar los riesgos del protocolo RFID.	66
6.3.2	Posibles aspectos a mejorar del estándar RFID.....	67
6.4	Mitigación de los riesgos y ataques en el protocolo NFC.....	67
6.4.1	Valoración personal de los métodos de mitigación NFC.....	68

6.4.2 Posibles aspectos a mejorar del estándar NFC.....	68
7. Conclusión	69
8. Bibliografía.....	70

1. Introducción

Los constantes avances en el ámbito de las tecnologías inalámbricas, están suponiendo un continuo incremento en la velocidad de conexión a un precio cada vez más reducido. Todo ello, está provocando que cada vez la movilidad sea una actuación más extendida tanto en los entornos laborales como privados.

En los últimos años el paradigma de la evolución de las redes inalámbricas, ha sido el terminal móvil, que ha pasado de ser un mero teléfono, a convertirse en un dispositivo multifunción que ofrece al cliente una gran variedad de servicios tecnológicos de última generación.

Sin embargo, la principal ventaja de estas tecnologías, que es la conexión sin cables, requiere una serie de medidas específicas de seguridad, imprescindibles si valoramos la información de la que disponen los sistemas que ofrecen dichas tecnologías.

Por ello se han escogido 4 de los protocolos más extendidos en el ámbito empresarial y personal, tales como las conexiones WIFI (802.11), la tecnología Bluetooth implantada hace tiempo, la tecnología RFID menos publicada pero de uso muy extendido, y una de las últimas incorporaciones a las tecnologías inalámbricas de comunicación de corto alcance NFC (siglas de Near Field Communication).

El objetivo principal es realizar un estudio de los ataques y riesgos existentes a nivel de seguridad, e identificar y comparar soluciones que ofrece el mercado o el propio protocolo, para mitigar dichas amenazas.

Para ello, se llevará a cabo un análisis de cada protocolo a nivel tecnológico a partir del cual, se detallaran los principales ataques que está sufriendo el mismo y las respuestas que se están dando hasta el momento.

2. Introducción a las redes sin hilos

En los últimos años, el uso y desarrollo de tecnologías inalámbricas, tales como el WIFI, WIMAX, GSM, Bluetooth,... ha aumentado enormemente en nuestra sociedad.

El motivo principal de dicho crecimiento ha sido el incremento en la utilización de dispositivos móviles que mediante todas estas redes y aplicaciones han buscado la mejor forma de conexión a Internet.

Para ello, se han llevado a cabo grandes avances en determinados campos, tales como el ancho de banda, diseño, protección de datos, velocidad de navegación... todo ello destinado a la adaptación de dichas tecnologías al creciente auge de la sociedad.

Históricamente, podemos decir que la primera red de conexión móvil que apareció, fue la GPS, dicho dispositivo permitía una transmisión de datos aceptable, pero disponía de unas prestaciones muy reducidas.

No será hasta la aparición de las redes GPRS en Europa y EDGE en Estados Unidos, más conocidas como 2,5G, cuando podamos hablar propiamente de conexión a Internet móvil. Dichas redes proporcionaban un ancho de banda de unos 10 Kbps que permitían el desarrollo de la mayoría de aplicaciones existentes hasta el momento.

Posteriormente aparecieron las redes UMTS, más conocidas como 3G, que aunque proporcionaban un ancho de banda entorno a los 300 Kbps, no tuvieron una gran acogida por parte de los usuarios, en gran medida por la falta de promoción realizada por sus desarrolladores.

Por todo ello, varios operadores llevaron a cabo la modificación en el estándar HSDPA/HSUPA dando como resultado las redes actuales, conocidas como 3,5G. Dichos dispositivos permiten una mayor velocidad de conexión, junto con una asimetría en los enlaces de subida y bajada que hasta el momento, están dando respuesta a las necesidades de la mayoría de usuarios.

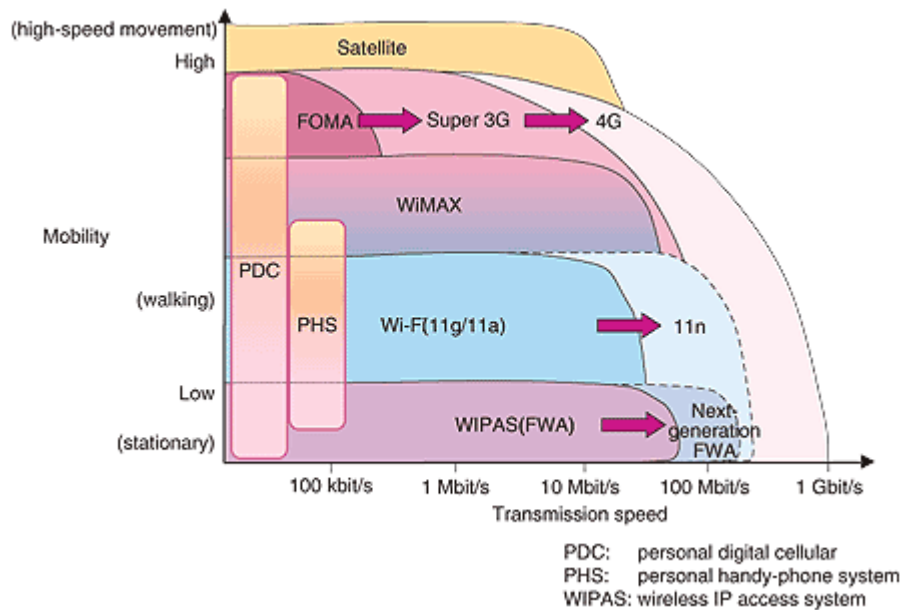
En base esto, han surgido nuevas problemáticas tales como la accesibilidad a la red, la velocidad de navegación, la seguridad en la red... que han hecho surgir nuevas tecnologías que tratan de evitar el colapso de las redes móviles y permiten a los usuarios un mejor servicio.

Entre dichas aplicaciones, encontramos 802.11g, RFID, NFC... que mediante una constante innovación, por parte de los operadores, están dando respuesta a las necesidades surgidas.

2.1 Tipos de redes sin Hilos

Cada una de las tecnologías citadas en el apartado anterior, disponen de una serie de características que las hacen más o menos adecuadas a las distintas aplicaciones, en función de la tecnología, el rango de cobertura y el de frecuencias utilizado para la transmisión.

En la siguiente imagen se pueden apreciar las tecnologías sin hilos en base a la movilidad y la velocidad de transmisión.



Si nos basamos en la **tecnología utilizada**, podemos distinguir entre:

- **Redes Inalámbricas de área personal:** Una red inalámbrica de área personal (WPAN) es aquella que abarca un área de algunas decenas de metros. Este tipo de red se usa generalmente para conectar dispositivos periféricos (por ejemplo, impresoras, teléfonos móviles y electrodomésticos) o un asistente personal digital (PDA) a un ordenador sin conexión por cables. También se pueden conectar de forma inalámbrica dos ordenadores cercanos. Se usan varios tipos de tecnología para las WPAN.

Dentro de este apartado encontraríamos las tecnologías de **Infrarrojos, Bluetooth, HomeRF y Zigbee.**

- **Infrarrojos.** Tecnología de redes de corto alcance, que no permiten la existencia de obstáculos entre los dispositivos que se comunican y con una baja velocidad de hasta 115 Kbps. Se utilizan principalmente en TV, PDAs, ordenadores portátiles, impresoras y teléfonos móviles.
- **Bluetooth.** Tecnología principal de las redes WPAN, lanzada por Ericsson en 1994. Ofrece una velocidad máxima de 1 Mbps con un alcance máximo de unos treinta metros. La tecnología Bluetooth, también conocida como IEEE 802.15.1, tiene la ventaja de tener un bajo consumo de energía, algo que resulta ideal para su uso en periféricos de tamaño reducido.
- **HomeRF (Home Radio Frequency):** Tecnología lanzada en 1998 por HomeRF Working Group (entidad que engloba a los fabricantes Compaq, HP, Intel, Siemens, Motorola y Microsoft, entre otros) que ofrece una velocidad máxima de 10 Mbps con un alcance de entre 50 y 100 metros sin amplificador. A pesar de estar respaldado por Intel, el estándar HomeRF se abandonó en enero de 2003, en gran medida porque los fabricantes de procesadores empezaron a usar la tecnología WIFI en placa (por medio de la tecnología Centrino, que incluía un microprocesador y un adaptador WIFI en un solo componente).

- **Zigbee:** Tecnología, también conocida como IEEE 802.15.4, que se utiliza para conectar dispositivos de forma inalámbrica con un coste y un consumo de energía muy bajo. Resulta particularmente adecuada dada su propiedad de integración directa en pequeños aparatos electrónicos, tales como, electrodomésticos, sistemas estéreos y juguetes. La tecnología Zigbee funciona en la banda de frecuencia de 2,4 GHz y puede alcanzar una velocidad de transferencia de hasta 250 Kbps con un alcance máximo de unos 100 metros.
- **Redes Inalámbricas de Consumo.** Una red inalámbrica de Consumo, es aquella que da servicio a un grupo de usuarios, ya sea de cantidad reducida (red local WIFI) o de hasta un millar de beneficiarios (red de comunicación móvil).

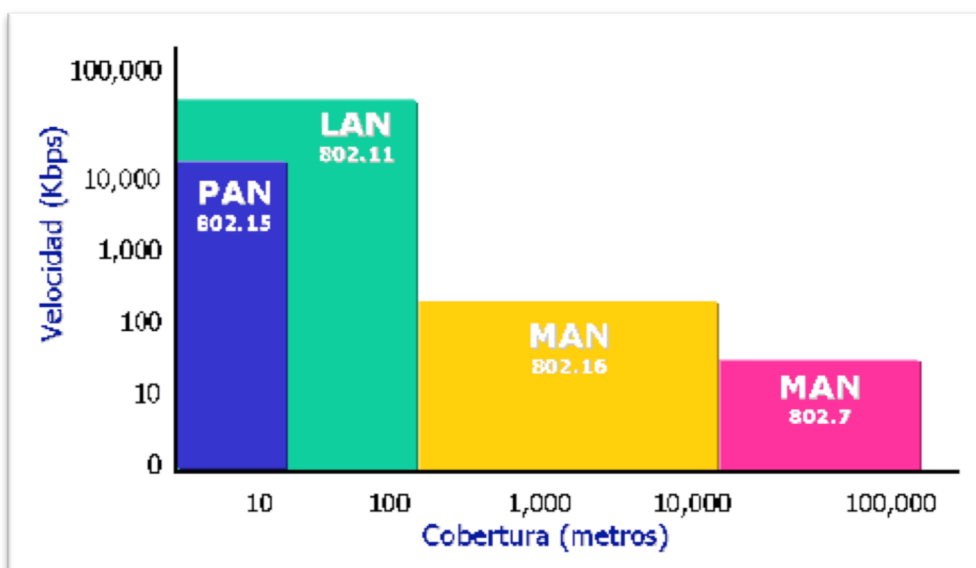
Dentro de este apartado encontraríamos las redes CDMA y GSM, la tecnología Wimax y las WLAN (Redes Inalámbricas de Área Local)

- **Redes CDMA, GSM, GPRS, 3G, UMTS.** Se trata de estándares de Comunicaciones Móviles. Son tecnologías inalámbricas que prestan servicios de voz de alta calidad, así como servicios de datos conmutados por circuitos en una amplia gama de bandas de espectro.
- **Wimax.** Se trata de redes inalámbricas de corto alcance, entre 3 y 10 Km, que se utilizan, principalmente, para ofrecer servicios de Banda Ancha a espacios con dimensiones de pocos kilómetros.
- **Redes Inalámbricas de Área Local.** Se trata de WLAN o redes WIFI que permiten el acceso a servicios de datos, tanto a dispositivos personales como empresariales.

Si nos basamos en el **rango de cobertura**, podemos distinguir entre:

- **WPAN.** (Wireless Personal Area Networks). Se trata de redes de uso personal, caracterizadas por su corto alcance. Entre dicha tipología, podemos destacar las redes ZigBee y Bluetooth.
- **WLAN.** (Wireless Local Area Network). Se trata de redes con un sistema de comunicación de datos más flexible que las redes LAN. Entre dicha tipología, podemos destacar las redes WI-FI y ZigBee.
- **WMAN.** (Wireless Metropolitan Area Networks). Se trata de redes de área metropolitana, con una cobertura de hasta 4 Km y basadas en el estándar IEEE 802.16. Entre dicha tipología, podemos destacar las redes LMDS y Wimax.
- **WWAN.** (Wireless Wide Area Network). Se trata de redes de área mundial, con una gran cobertura. Entre dicha tipología, podemos destacar las redes GPRS y UMTS.

En la siguiente imagen podemos ver un resumen de las redes en base a la velocidad y la cobertura:



Si nos basamos en el **rango de frecuencia**, podemos distinguir entre:

- **Ondas de radio.** Se encuentran entre bandas de frecuencia bajas que van desde ELF hasta UHF (3Hz – 3GHz). Para la propagación, utilizan antenas por el medio omnidireccional.
- **Microondas terrestres.** Se encuentran entre bandas de frecuencia que van desde 1 GHz hasta 300 GHz. Para la propagación, utilizan antenas parabólicas en enlaces punto a punto. Su principal inconveniente, es que los puntos a comunicar, deben estar perfectamente alineados.
- **Microondas por satélite.** Se encuentran entre bandas de frecuencia que van desde 1 GHz hasta 300 GHz. Para la propagación, utilizan un emisor de tierra que lanza una señal a un satélite encargado de amplificarla y enviarla a un receptor terrestre. Su principal inconveniente son las interferencias.
- **Infrarrojos.** Se encuentran entre bandas de frecuencia que van desde 300 GHz hasta 384 THz. Se utilizan en los equipos de visión nocturna cuando la cantidad de luz es insuficiente para ver los objetos, así como en dispositivos de control remoto. Su principal inconveniente es que entre emisor y receptor no puede haber ningún obstáculo.

2.2 Introducción al funcionamiento del estándar 802.11

2.2.1 Definición del estándar 802.11

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Lo único en lo que se diferencian es en la forma de transmitir las tramas o paquetes de datos.

Las principales características de la norma IEEE 802.11 son:

- Opera en las bandas de frecuencia 2.4 GHz y 5 GHz.
- Utilización de estaciones tipo computadores o dispositivos con interfaz inalámbrica.
- Utilización de radiofrecuencia o infrarrojos como medio de transmisión.

- Puntos de acceso con funcionalidad de “puentes” que se encargan de conectar dos redes con niveles de enlaces parecidos o distintos, mediante las conversiones de trama pertinentes.
- Sistema de distribución encargado de controlar donde se encuentran las estaciones para enviar las tramas.
- Conjunto de servicio básico, fundamentado en la intercomunicación de varias estaciones de forma directa o mediante la existencia de un punto de acceso.
- Conjunto de servicio extendido, fundamentado en la unión de varios BSS.
- Límite de red difuso, dada la opción de conexión de varios BSS.

El estándar original de este protocolo, data de 1997. Se conoció como IEEE 802.11 y no tuvo apenas relevancia dada la baja velocidad binaria alcanzada y la carencia de medidas de seguridad.

La siguiente modificación apareció en 1999 y se designó como IEEE 802.11b. Dicha especificación tenía velocidades de entre 5 y 11 Mbps y trabajaba en la frecuencia de 2,4 GHz.

A continuación, se realizó una especificación sobre una frecuencia de 5 GHz que alcanzaba los 54 Mbps, conocida como 802.11a que resultó incompatible con los productos de la b.

Posteriormente se incorporó un estándar a esa velocidad y compatible con el b que recibiría el nombre de 802.11g, y que al igual que la “b” utilizó la banda de los 2,4 GHz pero aumentando la velocidad de transmisión hasta los 54 Mbps.

Dado que convivían en el mercado tres especificaciones diferentes e incompatibles, el siguiente paso, fue crear equipos capaces de trabajar con las tres.

Para ello, se aprobaron nuevos estándares tales como el 802.11i que mejoraba la seguridad de las comunicaciones mediante el uso del Temporal Key Integrity Protocol. El 802.11e que permitía el envío de vídeo y voz sobre IP y realizaba el papel de árbitro en la comunicación y el 802.11h, entre otros, que permitía la asignación dinámica de canales para la coexistencia de éste con el HyperLAN.

En la actualidad, estamos inmersos en la especificación 802.11n que trabaja en la frecuencia de los 2,4 GHz, a una velocidad de 108 Mbps y se denomina Draft-N.

En la siguiente imagen se realiza un resumen de las principales especificaciones del 802.11n.

Normas (capa física y de acceso al medio)	Velocidad transmisión máxima (Mbps)	Throughput máximo típico (Mbps)	Numero máximo de redes colocalizadas	Banda de frecuencia	Radio de cobertura típico (interior)	Radio de cobertura típico (exterior)
IEEE 802.11a/h	54 Mbps	22 Mbps	14 (5.7 GHz)	5 GHz	85 m	185 m
IEEE 802.11b	11 Mbps	6 Mbps	3	2.4 GHz	50 m	140 m
IEEE 802.11g	54 Mbps	22 Mbps	3	2.4 GHz	65 m	150 m
IEEE 802.11n (40 MHz)*	>300 Mbps	>100 Mbps	1 (2.4 GHz) 7 (5.7 GHz)	5 GHz	120 m	300 m
IEEE 802.11n (20 MHz)*	144 Mbps	74 Mbps	3 (2.4 GHz) 14 (5.7 GHz)	2.4 GHz y 5 GHz	120 m	300 m

2.2.2 Principales usos del estándar 802.11

La tecnología 802.11, se utiliza principalmente en hoteles, aeropuertos, estaciones de servicio, centros de convenciones... ofreciendo acceso a Internet.

También se utiliza en el ámbito empresarial y residencial para la construcción de redes de área local inalámbricas.

Por último, también permite sustituir redes de telefonía celular en aquellas áreas donde no hay cobertura, entre otros muchos usos.

2.2.3 Descripción del funcionamiento de 802.11

El estándar 802.11, se compone de varios tipos de tramas que se clasifican en:

- **Management Frames.** Son aquellas tramas encargadas de gestionar la conexión a la red.

Dentro de este tipo de tramas, encontramos:

- Beacons.
- Probe Request
- Probe Response
- Association Request
- Association Response
- Authentication Request
- Authentication Response
- Deauthentication
- Reassociation Request
- Reassociation Response
- Announcement Traffic Indication Message (ATIM)

Primeramente, cabe destacar que las redes WIFI utilizan como política de acceso a la red la “*Carrier Sense Multiple Acces / Collision Avoidance*” mediante la cual, no se permite emitir y recibir a la vez por una misma antena. De este modo, se evita la aparición de las típicas colisiones de Ethernet que son imposibles de detectar de otro modo.

En referencia al funcionamiento, éste se desarrolla mediante el anuncio de la Infraestructura de red por parte de las tramas de “*Beacons*” que del mismo modo facilitan datos sobre ella, tales como, el ratio de transferencia de información, la potencia de transmisión, la autenticación,...

Una vez las estaciones reciben dichas tramas, ya disponen de la información necesaria de la red, para poder llevar a cabo la conexión. En aquellos casos, donde los “*Beacons*” se ocultan por motivos de seguridad las estaciones pueden escanear dichas redes para obtener la información necesaria, a partir de las “*Probe Request*” y las “*Probe Response*”.

Para iniciar la conexión, la estación envía una petición de acceso, mediante una “Association Request” y una “Authentication Request”, a la que la Infraestructura responde con una confirmación de acceso, mediante una “Association Response” y una “Authentication Response”.

Una vez realizada la autenticación y la asociación, el cliente puede abandonar parcialmente la red, mediante la trama “Deauthentication”, quedando desligado el proceso de asociación, pero no el de autenticación. De modo que, en caso que la estación quiera retomar dicha conexión, únicamente serán necesarias las tramas de asociación “Reassociation Request” y “Reassociation Response”.

En cuanto a las tramas de “Announcement Traffic Indication Message”, cabe indicar, que éstas son utilizadas para avisar a los “peers” de la existencia de datos pendientes en las redes WIFI Ad-Hoc.

- **Control Frames.** Son aquellas tramas encargadas de gestionar el modo de acceder al medio.

Dentro de este tipo de tramas, podemos encontrar:

- **DCF. Distributed Coordination Function.**

Este modo de acceso, utiliza las tramas de control RTS “Request To Send”, CTS “Clear to Send” y Ack.

En primer lugar, la estación envía una petición de acceso, mediante un RTS que es confirmado por la misma, a través de un CTS. A partir de aquí, se realiza la transmisión de los datos y la Infraestructura confirma la recepción de éstos, mediante un ACK.

- **PCF. Point Coordination Function.**

Este modo de acceso, utiliza las tramas de control CF+End, CF+End_Ack_, CF-Ack, CF-Ack+CF-Poll y CF-Poll.

En primer lugar, un Punto de Acceso toma el control del medio y a partir de aquí gestiona los accesos de las estaciones a la Infraestructura, mediante las tramas CF-Poll y CF-Ack (solicitud de permiso de transmisión y reconocimiento de la misma).

El punto de acceso, también es el encargado de marcar la velocidad de transmisión obligatoria a la que las estaciones deben funcionar, junto con el control del tráfico de datos que circula por la misma.

De todos modos, es muy común encontrar esquemas de funcionamiento mixtos, es decir, en los que se utilicen tramas DCF y PCF en diferentes periodos de tiempo.

- **Data Frames:** Un Data Frame de 802.11 consta de un campo de control de trama, campos de dirección, cuerpo de bastidor, y el campo de secuencia de verificación de trama. El campo de control de trama tiene la misma estructura que otras tramas 802.11. El tipo subcampo del campo de control que distingue a la trama de datos de otros marcos.

2.2.4 Medidas de seguridad 802.11

Si nos basamos en las medidas de seguridad que se pueden aplicar en la redes 802.11, podemos destacar las siguientes características:

- **Redes Abiertas.** Caracterizadas por no tener implementado ningún sistema de autenticación o cifrado. En ellas, las comunicaciones entre los terminales y los AP viajan en texto plano y no se solicita ningún dato para acceder a ellas. Como actuaciones que puedan garantizar en mayor medida la seguridad en estas redes, encontramos:

- **Filtrado por MAC o IP.** Sistema que permite el acceso sólo a aquellas terminales que hayan sido previamente configuradas en el AP mediante ACL.

Para ello, se utilizan las denominadas *Listas de Control de Acceso (ACL –Access Control List)* basadas en MAC. Dicha medida, consiste en la creación de una lista con aquellas direcciones MAC de los equipos a los que se les permite el acceso a red.

Actualmente, quebrantar dicha limitación resulta sencillo, a partir de la sustitución de una tarjeta que contenga la dirección MAC, por otra válida obtenida mediante un Sniffer.

- **Bloqueo de Beacon Frames.** Sistema que bloquea el envío de Beacon Frames para evitar que se conozca el ESSID.

Durante mucho tiempo se aconsejó ocultar el ESSID de una red, para de ese modo resultar “invisible” a posibles intrusos. Pero en la actualidad, la mayoría de los dispositivos disponen de la opción de “búsqueda de redes ocultas”, que permite visualizar aquellas con el ESSID deshabilitado. De igual forma, éste puede ser obtenido mediante la captura de alguna conexión, realizada por un Sniffer a través de las tramas “*Probe Request*” o “*Probe Response*”.


Estas medidas tienen como objetivo, limitar el acceso al sistema a usuarios no autorizados, pero, no suponen ningún impedimento en cuanto a aquellas acciones de espionaje que se puedan producir en las comunicaciones.

- **Redes Cerradas.** Caracterizadas por aplicar protocolos de cifrado de datos que se encargan de codificar la información que se transmite y así, garantizar su confidencialidad.

Dentro de estos protocolos cabe señalar:

- **WEP.** Dicho protocolo, mediante la utilización de una clave, cifra los datos antes de enviarlos al aire, de modo que, tan sólo pueda acceder a ellos el destinatario deseado. Puede realizar cifrados de 64 o 128 bits.
- **WPA.** Dicho protocolo, introduce como modificación respecto al anterior, el hecho que la clave, esté constituida por dígitos alfanuméricos.
- **WPA2.** Dicho protocolo es una mejora del WPA puesto que requiere hardware y software compatibles y actualmente, es el más utilizado en redes 802.11.

En la siguiente imagen se relacionan las principales características de los protocolos anteriormente descritos.



	Security Type	
Encryption	WEP128	STANDARD
	CKIP (Cisco TKIP)	STANDARD
	CMIC (Cisco MIC)	STANDARD
802.1X Authentication	LEAP	STANDARD
	PEAP-MSCHAPv2	STANDARD
	PEAP-GTC	STANDARD
	EAP-FAST	STANDARD
WPA (WI-FI Protected Access)	WPA-PSK (Pre-Shared Key)	STANDARD
	LEAP (WPA)	STANDARD
	PEAP-MSCHAPv2 (WPA)	STANDARD
	EAP-FAST (WPA)	STANDARD
	EAP-TTLS (WPA)	STANDARD
	EAP-TLS (WPA)	STANDARD
WPA 2	AES	STANDARD

Como se puede observar en la imagen anterior, es necesario hacer hincapié en los protocolos de control de acceso 802.1X y el protocolo WPA2 (WI-FI Protected Access).

El **protocolo 802.11x**, cuya función principal es encapsular los protocolos de autenticación sobre los de la capa de enlace de datos (capa 2 del modelo OSI) la cual se encarga de describir el modo de autenticación basado en EAP (Extensible Authentication Protocol).

Dicho sistema, define tres elementos:

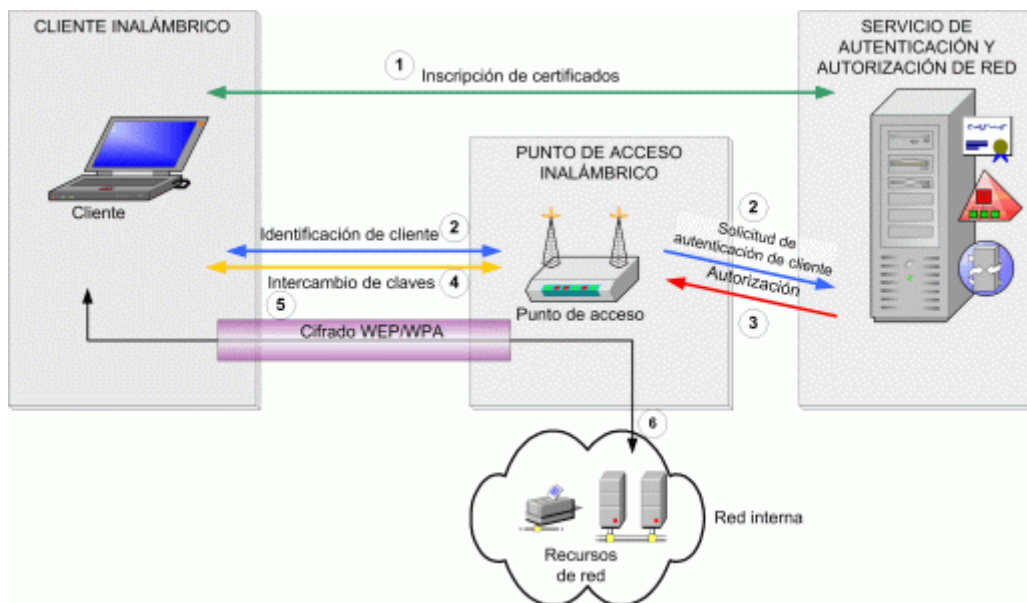
- **Solicitante o suplicante.** Elemento encargado de solicitar la autenticación. Generalmente, se trata del cliente.
- **Autenticador.** Elemento encargado de pasar la información al servidor de autenticación, y al que se conectará el suplicante. Generalmente, se trata del Punto de Acceso.
- **Servidor de autenticación.** Elemento encargado de evaluar la legalidad del suplicante y enviar una respuesta al autenticador. Generalmente, se trata del servidor *Radius*.

El sistema EAP, no es un propiamente un mecanismo de autenticación, sino una estructura de soporte que puede transportar diferentes protocolos de autenticación, tales como TLS (Transport Layer Security), TTLS (Tunnel Transport Layer Security), MD5 (Message Digest 5), PEAP (Protected EAP), LEAP (Lightweight EAP), etc...

El sistema EAP-TLS se basa en la utilización de certificados digitales X.509 para la autenticación de cliente y servidor. El principal inconveniente del mismo, es que tanto

unos como otros, deben poseer certificado digital propio, hecho que supone una gran dificultad en cuanto a la distribución de los mismos entre un gran número de clientes y el elevado coste de los mismos. Es por eso que se creó PEAP y EAP, dado que únicamente requerían certificado en el servidor.

En la siguiente imagen se puede observar la estructura básica de la autenticación por EAP y PEAP.



El sistema EAP-TTLS añade a las características de seguridad del anterior, un canal de comunicación seguro para intercambiar credenciales con el usuario, reduciendo enormemente los ataques de Sniffing. De igual forma, elimina la necesidad de contar con certificados en todos los clientes.

Los tipos de mensajes de intercambio, son los siguientes:

- **Request.** Petición desde el Punto de Acceso al Cliente.
- **Response.** Mensaje del cliente al Punto de Acceso.
- **Success.** Autorización de acceso.
- **Failure.** Denegación de acceso.

El transporte de los mensajes, se lleva a cabo, a través del protocolo *Ealpol (Eal over LAN)*, desarrollado para entornos Ethernet y en el que se pueden encontrar cinco tipos de mensajes:

- **Start.** El cliente envía la solicitud de acceso, mediante la dirección MAC multicast, y espera que el Punto de Acceso responda.
- **Key.** El Punto de Acceso envía las claves al Cliente, una vez autorizada la entrada del mismo.
- **Packet.** Los mensajes *EAL* que son transmitidos, se encapsulan en este mensaje *EALPOL*.
- **Logoff.** El cliente envía un mensaje de desconexión.
- **Encapsulated-ASF-Alert.** Actualmente no se utiliza.

El funcionamiento estándar del protocolo 802.11x se basa en el rechazo de todo el tráfico que no vaya dirigido al servidor de autenticación, hasta que el cliente no es autorizado. El autenticador genera un puerto por cliente con dos opciones: autorizado o

no. Dicho puerto se mantendrá cerrado hasta la verificación de acceso del cliente.

Una vez el solicitante tiene acceso autorizado, éste se asocia a un AP. Cuando el autenticador detecta dicha asociación, le habilita un puerto permitiendo el tráfico y bloqueando el resto.

El cliente envía el mensaje “EAP Start” al que el autenticador responde con un “EAP Request Identity” para obtener la identidad del mismo. Éste le envía un “EAP Response” donde le indica su identificador, el cual es retransmitido por el autenticador hacia el servidor de autenticación. A partir de entonces, el solicitante y el servidor de autenticación se comunican directamente.

Después de presentar el protocolo 802.1x, es necesario hacer hincapié en el WPA2.

Dicho protocolo tiene dos modos de funcionamiento:

- **WPA2-ENTERPRISE.** basado en el protocolo 802.1x explicado anteriormente, que utiliza los tres elementos ya descritos (suplicante, autenticador, servidor de autenticación).
- **WPA2-PSK (Pre-Share Key).** Pensado para ser utilizado en entornos personales, el cual, se encarga de evitar el uso de dispositivos externos de autenticación.

Tanto el servidor de autenticación como el suplicante, durante la fase de autorización y autenticación de 802.11x, generan dos claves aleatorias denominadas PMK (Pairwise Master Key). Una vez finalizada dicha fase, el servidor de autenticación y el cliente tienen PMK idénticas, pero el Punto de Acceso no, por lo tanto a través del uso de RADIUS se llevará a cabo la copia de la clave. El protocolo no especifica el método de envío de la clave entre ambos dispositivos.

A continuación, generarán nuevas claves, en función de la PMK, para ser utilizadas en relación al cifrado y la integridad. Dichas combinaciones formaran un grupo de cuatro denominado PTK (Pairwise Transient Key) con una longitud de 512 bits.

Con la finalidad de asegurar el tráfico broadcast, se crean claves de grupos de 256 bits llamadas GMK (Group Master Key) utilizadas para crear la GEK (Group Encryption Key) y la GIK (Group Integrity Key) de 128 bits de longitud cada una. En este caso, las cuatro claves formaran la GTK (Group Transient Key).

Por último, se debe demostrar que el Punto de Acceso dispone de PMK idéntico, para ello se lleva a cabo una validación mediante el servidor de autenticación. Dicho proceso se realiza cada vez que se asocia un cliente con un Punto de Acceso.

Sin embargo, cabe destacar que todos los métodos de seguridad detallados hasta el momento son susceptibles de ser vulnerados.

Tabla resumen de las medidas de seguridad:

Medida de seguridad	Principales características
WEP (Wired Equivalent Privacy o Privacidad Equivalente al Cable)	Fue el primer sistema de cifrado asociado al protocolo 802.11. WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. El algoritmo de encriptación utilizado es RC4 con claves (seed). Se considera como el menos seguro de todos por su

	facilidad para romperlo
WPA (Wi-Fi Protected Access o Protección de Acceso Wi-Fi).	Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autenticación. WPA incluye IEEE 802.1X, EAP, TKIP, MIC. Tiene dos modos de funcionamiento Con servidor AAA y con Clave inicial compartida (PSK).
WPA2 (Wi-Fi Protected Access o Protección de Acceso Wi-Fi, versión 2)	Esta basado en el WPA. WPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS
Ocultación Red 802.11	Cambiar el SSID por defecto y desactivar el Broadcasting SSID.
Activación del filtro MAC	Permitir el acceso a través de los AP sólo a los sistemas permitidos, mediante listas blancas en los AP o controladores WI-FI, filtrando a nivel de enlace.
Tipos de autenticación (802.11X) – EAP	Protocolo extensible de autenticación. Es un protocolo que sirve para adaptar a las redes inalámbricas protocolos ya establecidos y otros nuevos.
Tipos de autenticación (802.11X) – EAP-MD5	Mediante EAP se autentifica realizando un intercambio de claves "cifradas" por MD5. Las credenciales puede ser nombre de usuario y contraseña o una dirección MAC.
Tipos de autenticación (802.11X) – EAP-TLS	La autenticación se realiza mutuamente mediante certificados. Con este sistema tanto el ACS como el cliente deben demostrar su identidad.
Tipos de autenticación (802.11X) – PEAP	Es un estándar del IETF basado en contraseña secreta. Requiere un certificado en el servidor de autenticación. Este certificado se envía al cliente, el cual genera una clave de cifrado maestra y la devuelve cifrada utilizando la clave pública del servidor de autenticación.

2.3 Introducción al funcionamiento del estándar Bluetooth

2.3.1 Definición del estándar Bluetooth

En 1994 la empresa sueca Ericsson inició un estudio para investigar la viabilidad de un interfaz vía radio, de bajo coste y consumo, para la interconexión entre teléfonos móviles y otros accesorios, con el objetivo de eliminar cables entre aparatos.

Dicho estudio partía de un proyecto anterior sobre multicomunicadores conectados a una red celular, y que cuando llegó a un enlace de radio de corto alcance se denominó MC link.

A medida que avanzaba el proyecto, se ponía de manifiesto que dicho enlace podía ser utilizado en un gran número de aplicaciones, dado lo económico del chip en el que se basaba.

A principios de 1997, varios fabricantes de equipos portátiles que mostraron interés por el avance del proyecto e incluyeron dicha tecnología en el diseño de los equipos.

Ello fue lo que originó a principios de 1998, la creación de un Grupo de Especial Interés en Bluetooth (SIG) formado por cinco promotores (Ericsson, Nokia, IBM, Toshiba e Intel) con el objetivo de lograr un conjunto adecuado de áreas de negocio. Hay que tener en cuenta, que en el grupo se hallaban dos líderes del mercado de las telecomunicaciones, dos del mercado de las PCs portátiles y un líder de fabricación de chips.

Actualmente el SIG cuenta con miembros tan importantes como Motorola, 3Com, Lucent y Microsoft, el respaldo de 1900 empresas de tecnología y 2000 empleados de otras tantas empresas que investigan productos y servicios con aplicaciones Bluetooth.

Hasta la actualidad, se han producido tres grandes variaciones de Bluetooth:

- La primera versión, no tenía seguridad esencial, era lenta y propensa a las interferencias.
- La segunda, lanzada en el 2004 disponía de una mayor velocidad de transferencia de información con un bajo consumo, y reforzaba los aspectos de seguridad.
- La última versión, aprobada por el SIG en 2009 suponía un aumento de la velocidad de transferencia de hasta 24 Mbit / sg y ello se lograba mediante la combinación de tecnología Bluetooth y tecnología 802.11.

Bluetooth es un estándar de comunicación para redes inalámbricas personales, que permite la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia en entornos de comunicaciones móviles y estáticas.

Sus principales características son:

- Dispositivos de bajo consumo.
- La frecuencia en la que opera es de 2.4 GHz.
- Redes de corto alcance tipo Adhoc.
- Bajo coste de implementación.
- Conexión sin cables vía OBEX.
- Sistema basado en un protocolo robusto y seguro.
- Posibilidad de conexión entre una gran tipología de dispositivos.
- Velocidad de transmisión que puede llegar a 3 Mbps.

2.3.2 Principales usos del estándar Bluetooth

La tecnología Bluetooth, se utiliza principalmente en conexiones inalámbricas.

También para realizar el traspaso de archivos de un dispositivo a otro. Nos permite acceder a Internet mediante telefonía móvil o un módem inalámbrico.

Del mismo modo, podemos eliminar el cableado de los equipos informáticos, tanto del teclado, como del ratón...

Y por último, lo podemos utilizar en el coche como dispositivo de manos libres, entre otros muchos usos.

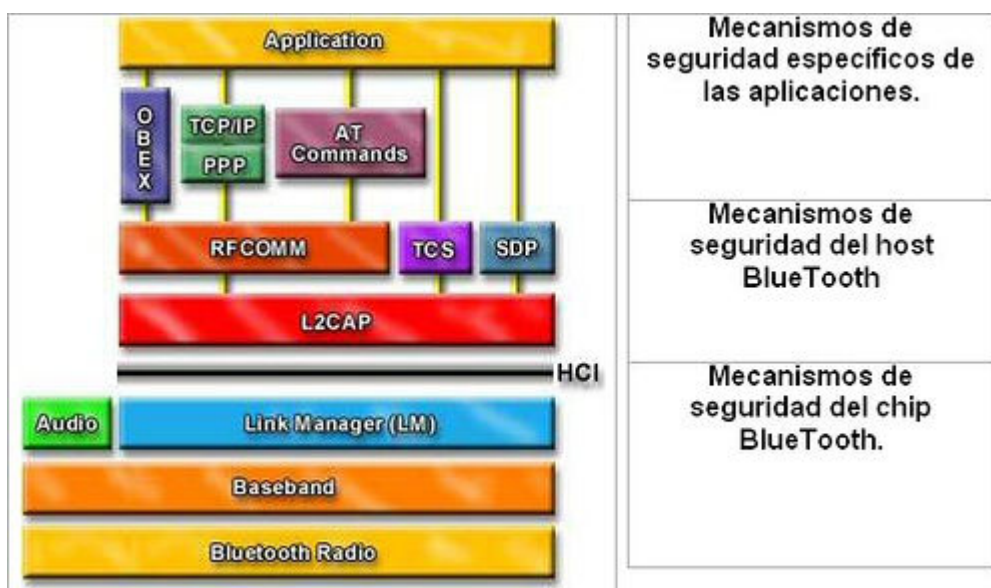
2.3.3 Descripción del funcionamiento de Bluetooth.

La especificación de Bluetooth pretende que todas las aplicaciones sean capaces de operar entre sí. Para conseguir esta interoperabilidad, las aplicaciones en dispositivos remotos deben ejecutarse sobre una pila de protocolos idénticos.

En la comunicación con otros dispositivos, se requiere un hardware específico para Bluetooth, que incluye un módulo de banda base, así como otro de radio y una antena. Además deberá haber un software encargado de controlar la conexión entre dos dispositivos Bluetooth; el cual por lo general correrá en un microprocesador dedicado. Los Link Managers de diferentes dispositivos Bluetooth se comunicarán mediante el protocolo LMP (Link Manager Protocol).

De igual forma, habrá otros módulos de software, que constituirán la pila de protocolos, y garantizarán la interoperabilidad entre aplicaciones alojadas en diferentes dispositivos Bluetooth.

En la siguiente imagen se muestra la pila de protocolos del bluetooth.



La pila completa se compone tanto de protocolos específicos de Bluetooth (Link Manager, L2CAP Logical Link Control Adaption Protocol...), como de protocolos no específicos (OBEX Objects Exchange Protocol, UDP User Datagram Protocol, TCP, IP, etc) dado a que la hora de diseñar la torre de éstos, el objetivo principal ha sido maximizar el número de protocolos existentes que se puedan reutilizar con diferentes propósitos, en las capas más altas-

Además, la especificación define el HCI (Host Controller Interface), encargado de proporcionar una interfaz de comandos al controlador BaseBand y proporcionar el acceso al estado del hardware y a los registros de control.

Las redes Bluetooth, se caracterizan por ser sistemas basados en continuos saltos de frecuencia “*Frequency hopping*” con el fin de evitar interferencias y reducción de la señal transmitida.

Mediante la cabecera de cada uno de los pequeños paquetes que se transmiten, se indica, entre otros datos, la frecuencia de la banda en la que se enviará el siguiente paquete; de este modo se producen los saltos de frecuencia indicados, en función del tráfico de la red y otros factores.

Estas redes están preparadas para interconectar hasta ocho periféricos entre sí, es lo que se conoce como “*Piconet*”. Para el buen funcionamiento de este sistema, se sincroniza un reloj global y un patrón de saltos específico.

Se marca uno de los dispositivos como “maestro”, el resto, serán “esclavos”, y éste es el encargado de regular el tráfico mediante un reloj interno y su dirección única. De este modo, se marca el patrón de saltos en base a una permutación aleatoria de 79 frecuencias en la banda ISM.

Cada “maestro”, puede estar conectado a dos “*Piconets*” distintas, y como puede haber varios maestros en una misma red, se pueden interconectar varias “*Piconets*” entre sí de forma encadenada, hasta un máximo de 10, es decir, un total de 72 periféricos.

Hay 20 perfiles que se encargan de controlar el comportamiento del periférico Bluetooth, de los cuales sólo 13 se utilizan hoy en día. Lo correcto, sería que todos los periféricos dispusieran de la totalidad de los perfiles, pero esto supone un incremento del coste del chip, por lo que no siempre es así.

También encontramos 3 tipos de enlaces distintos, que asignan los modos de transmisión entre dispositivos. La elección de los mismos, depende de la naturaleza del tráfico.

Podemos distinguir entre:

- **Enlaces síncronos.** Permiten una conexión bidireccional a 432 Kbps en cada sentido que los hace ideales para intercambio de datos entre equipos.
- **Enlaces asíncronos.** Ofrecen 721 Kbps en un sentido y 57.6 Kbps en el otro, que los hace más adecuados para periféricos que reciben gran cantidad de datos, pero envían pocos.
- **Enlaces de voz/datos.** Ofrecen un canal bidireccional a 64 Kbps garantizados, permitiendo la fluidez necesaria para una transmisión de audio.

2.3.4 Medidas de seguridad Bluetooth

Si nos basamos en la tipología de seguridad aplicada a la tecnología Bluetooth, podemos distinguir entre tres modos primarios:

- **Modo 1. Sin seguridad .** Todos los mecanismos de seguridad (autenticación y cifrado) están deshabilitados. Además el dispositivo se sitúa en modo promiscuo, permitiendo que todos los dispositivos Bluetooth se conecten a él.

- **Modo 2. En la capa L2CAP, nivel de servicios .** Los mecanismos de seguridad son inicializados después de establecerse un canal entre el nivel LM y el L2CAP. Un gestor de seguridad es el encargado de controlar el acceso a servicios y dispositivos. Variando las políticas de seguridad y los niveles de confianza se pueden gestionar los accesos de aplicaciones con diferentes requerimientos que operen en paralelo. Su interface es muy simple y no hay ninguna codificación adicional de PIN o claves.
- **Modo 3. En el nivel de Link.** Los mecanismos de seguridad son iniciados antes de establecer un canal. Todas las rutinas están dentro del chip BlueTooth y nada es transmitido en plano. Aparte del cifrado tiene autenticación PIN y seguridad MAC. Su metodología consiste en compartir una clave de enlace secreta entre dos dispositivos, la cual se genera mediante el procedimiento de “pairing” cuando dichos dispositivos se comunican por primera vez.

Como actuaciones que puedan garantizar en mayor medida la seguridad en estas redes, encontramos:

- **Solicitud código PIN.** Consiste en el requerimiento de autenticación por parte de varios dispositivos Bluetooth para realizar una determinada operación.

El código PIN es una cadena ASCII formada por hasta 16 caracteres, que el usuario debe introducir en los diferentes dispositivos a utilizar, para que éstos generen una clave de enlace. Adicionalmente para realizar la comunicación en bluetooth es necesario emparejar los dispositivos. Por defecto, la comunicación Bluetooth no se valida, por lo que cualquier dispositivo puede en principio hablar con cualquier otro. Un dispositivo Bluetooth (por ejemplo un teléfono celular) puede solicitar autenticación para realizar un determinado servicio (por ejemplo para el servicio de marcación por modem).

La autenticación de Bluetooth normalmente se realiza utilizando códigos PIN. Un código PIN es una cadena ASCII de hasta 16 caracteres de longitud. Los usuarios deben introducir el mismo código PIN en ambos dispositivos.

Una vez que el usuario ha introducido el PIN adecuado ambos dispositivos generan una clave de enlace. Una vez generada, la clave se puede almacenar en el propio dispositivo o en un dispositivo de almacenamiento externo. La siguiente vez que se comuniquen ambos dispositivos se reutilizará la misma clave.

El procedimiento descrito hasta este punto se denomina emparejamiento (pairing). Es importante recordar que si la clave de enlace se pierde en alguno de los dispositivos involucrados se debe volver a ejecutar el procedimiento de emparejamiento.

No existe ninguna limitación en los códigos PIN a excepción de su longitud. Algunos dispositivos (por ejemplo los dispositivos de mano Bluetooth) pueden obligar a escribir un número predeterminado de caracteres para el código PIN.

- **Solicitud claves de cifrado.** Consiste en el requerimiento de una clave generada mediante la aplicación del algoritmo E3, que corresponde a un número aleatorio de 128 bits y un Ciphering Offset (COF) basado en el valor de ACO del proceso de autenticación. De este modo, los datos transmitidos, sólo pueden ser recibidos por el usuario autorizado.

Tabla resumen de las medidas de seguridad:

Medida de seguridad	Principales características
Modos de Seguridad	<p>Modo 1: Permite conexiones desde cualquier dispositivo.</p> <p>Modo 2: Requiere una seguridad sencilla por servicio. L2CAP</p> <p>Modo 3: Utiliza procedimientos de seguridad:</p> <ul style="list-style-type: none"> • Uso de autenticación • Filtrado por dirección de origen (BD_ADDR) • Cifrado mediante SAFER+
Seguridad en Autenticación – PIN	Utilización de un PIN entre 4 y 16 dígitos
Claves utilizadas en el “Paring”	<p>Kx – Clave de cada dispositivos, se genera una sola vez.</p> <p>Kinit – Clave inicial necesaria para realizar los siguientes pasos.</p> <p>Klink – Clave temporal de enlace</p>
Cifrado de datos	En la transmisión los datos se cifran con el algoritmo XOR (BD_ADDR, Hora del sistemas, Kc)

2.4 Introducción al funcionamiento del RFID

2.4.1 Definición del estándar RFID

RFID (Radio Frequency Identification) es un estándar de comunicación mediante radiofrecuencia, que se encarga del almacenamiento y recuperación de datos mediante el uso de dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID.

Dichos dispositivos, son similares a una pequeña pegatina que se adhieren a objetos, animales o personas, y contiene antenas que permiten recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID.

El origen de la tecnología RFID, se remonta al 1946, cuando León Theremin desarrolló una herramienta de espionaje para identificar aeroplanos, consistente en un sistema de escucha pasivo para la Unión Soviética. Dicho dispositivo retransmitía ondas de radio incidentes con información de audio y supuso la base de los actuales sistemas RFID activos.

En 1973, Charles Watson patentó la tecnología RFID pasiva, para cerraduras de puertas. Dicha tecnología pronto se extendió a lectores de carnets y aplicaciones de control de asistencia.

A partir de 1979, se utilizó la tecnología RFID en identificación y seguimiento de animales. En 1994, los ferrocarriles de Estados Unidos utilizaban tags de RFID para identificación.

Actualmente, la reducción del coste de dicho sistema gracias a los avances en la fabricación de semiconductores, ha supuesto el auge de dicha tecnología y la aplicación de la misma en sectores donde la reutilización de los tags imposible hasta ese momento.

Sus principales características son:

- No es necesaria la conexión visual entre emisor y receptor.
- Distancia de lectura de 1 a 10 metros.
- Flujo de información rápido. Identificación en menos de un segundo.
- Permite almacenar, leer, reescribir o agregar la información contenida.
- Los componentes necesarios son: lector, antenas, transpondedores y computadoras de almacenaje de datos.

2.4.2 Principales usos del estándar RFID

La tecnología RFID, se utiliza principalmente en sectores industriales para la realización del control de calidad, producción y distribución de objetos.

También permite la realización del inventario de una forma automática, llevar un control sobre las fechas de caducidad, evitar falsificaciones, localizar objetos...

Y por último, también permite la identificación y control de equipajes en aeropuertos, entre otras muchas utilidades.

2.4.3 Introducción al funcionamiento RFID

El funcionamiento del estándar de comunicación RFID, se basa en la utilización de un lector, antenas y una serie de transpondedores.

Los transpondedores son los encargados de contener los datos de identificación del objeto, animal o persona al que hacen referencia, y mediante la emisión de una señal de radiofrecuencia que puede ser captada por un lector RFID, llevar a cabo una verificación e intercambio de datos con el mismo que finalmente, pasan en formato digital a la aplicación específica que utiliza RFID para su procesamiento y gestión.

El sistema RFID se compone de tres dispositivos:

- **Lector de RFID o Transceptor.** Se compone de antena, transceptor y decodificador.
Mediante el envío periódico de señales, el lector trata de averiguar si hay alguna etiqueta en las inmediaciones. Cuando capta alguna señal emitida por un transpondedor, extrae la información y la pasa al subsistema de procesamiento de datos.
- **Middleware RFID.** Proporciona los medios necesarios para el proceso y almacenaje de la información registrada.
- **Etiqueta RFID o Transpondedor.** Se compone de antena, traductor radio y chip.

La antena permite al chip, que contiene la información, transmitirla mediante una señal de radiofrecuencia.

La memoria interna del chip, dependerá del modelo y su capacidad puede variar entre los 10 y los 1000 Bytes. En cuanto a la información contenida, podemos encontrar memorias de varios tipos:

- **Solo lectura:** contiene un código de identificación único y personalizado desde su fabricación.
- **De lectura y escritura:** contiene un código de identificación que puede ser modificado por el lector.
- **Anticolisión.** Son etiquetas que permiten al lector una identificación múltiple en un mismo tiempo.

2.4.4 Medidas de seguridad RFID

Como actuaciones que puedan garantizar en mayor medida la seguridad en estas redes, encontramos:

- **Utilización jaula Faraday.** Dicho dispositivo está compuesto por un conjunto de hilos metálicos entrecruzados que anulan el campo electromagnético, bloqueando la emisión de la antena RFID que podría ser captada por el lector RFID del infractor. De ese modo, los datos de los objetos que contenga esta jaula, no podrán ser interceptados.
- **Inutilización etiquetas RFID.** Consiste en la desactivación o destrucción de dichas etiquetas una vez finalizada su misión. De este modo, se elimina la información contenida en las mismas, evitando el acceso a la misma por parte de atacantes.
- **Eliminación información personal tags.** Consiste en la desactivación o destrucción de la información personal de las etiquetas una vez finalizada su misión. De este modo, se elimina la información contenida en las mismas, evitando el acceso a la misma por parte de atacantes.
- **Utilización técnica de cifrado.** Consiste en realizar una transcripción de la información transmitida, de forma que el personal no autorizado, no pueda acceder a los datos.
- **Solicitud clave secreta.** Consiste en el requerimiento de autenticación para validar la comunicación entre el lector al iniciar su utilización. De ese modo se evitan falsificaciones.
- Tabla resumen de las medidas de seguridad:

Medida de seguridad	Principales características
Utilización de técnicas de cifrado	Realizar un cifrado de comunicaciones para impedir el sniffing. Las técnicas de cifrado son creadas por los proveedores por ejemplo el MIFARE de Phillips.
Autenticación	Solicitud de una clave secreta compartida entre el lector y la etiqueta. Por ejemplo tendríamos el MIFARE.
Lecturas aleatorias	Etiquetas que tienen un conjunto de seudónimos,

	lo que impide la lectura de forma directa, si por fuerza bruta.
Etiquetas de un solo uso	Etiquetas que sólo se pueden leer una sola vez.
Etiquetas watchdog	Etiquetas que registran la actividad de lectura.

2.5 Introducción al funcionamiento del NFC

2.5.1 Definición del estándar NFC

Con la implantación de la tecnología RFID y el auge de la telefonía móvil se buscó la forma de incluir en ellos estos nuevos métodos de comunicación, con dicha finalidad, se depuraron varios aspectos, tales como, la reducción del alcance de la señal o el almacenaje de cierto tipo de datos.

En base a estas modificaciones, en 2002 nace el primer estándar bajo el nombre de mobile RFID o NFC, realizado por el organismo ECMA (ECMA-340). El 8 de diciembre de 2003, dicho estándar fue aprobado a nivel internacional como ISO/IEC 18092, incluyendo los estándares ISO 14443 (Tipos A y B) y FeLica.

El 18 de marzo de 2004, Nokia, Philips y Sony se asociaron y crearon el **NFC Forum** con la finalidad de seguir avanzando en el alcance de la tecnología NFC. Actualmente, dicho organismo ha elaborado varias especificaciones, las más importantes de las cuales son NFCIP-1 y 2 que definen el protocolo de comunicación entre dos dispositivos NFC y promueven el logotipo N Mark como distintivo de dicha tecnología.

Sus principales características son:

- No es necesario el contacto directo entre el dispositivo emisor y el receptor.
- Utilización del protocolo ISO 14443.
- Opera en la frecuencia 13.56 MHz, banda que no necesita licencia administrativa para transmitir.
- Realización de operaciones a una distancia inferior a 10 centímetros.
- Velocidad de transmisión que va de los 106 Kbit/sg hasta los 424 Kbit /sg

2.5.2 Principales usos del estándar NFC

La tecnología NFC, se utiliza principalmente en anuncios inteligentes o SmartPosters, mediante las etiquetas de los cuales, embebidas en carteles, anuncios, logotipos, etc... se accede a sitios web con múltiples campañas publicitarias.

También permite la configuración de dispositivos y aplicaciones, de modo que acciones que se llevan a cabo frecuentemente y que podrían representar una gran pérdida de tiempo para el usuario, tales como configurar el despertador, bajar el volumen de las llamadas por la noche... mediante la conformación de comandos de control genérico y URIs almacenadas en etiquetas NFC, son activadas con el simple hecho de acercar el dispositivo.

Por último, también permite la realización de Pago móvil NFC, igual que realizarías con una tarjeta de crédito.

2.5.3 Introducción al funcionamiento NFC

El funcionamiento del estándar de comunicación NFC, se caracteriza por varios aspectos básicos:

- **Comunicación inalámbrica por proximidad.** Este tipo de comunicación, similar al de otras tecnologías como tarjetas inteligentes, se realiza mediante el uso de inducción electromagnética. Los dispositivos compatibles con NFC deben contar con una pequeña antena en espiral que genera un campo electromagnético de radiofrecuencia. Cuando un dispositivo entra en el campo electromagnético de otro, se puede establecer comunicación entre ellos. El alcance de dicho campo es muy pequeño, de unos cuatro centímetros, aproximadamente. Hecho que supone, que los dispositivos necesiten casi entrar en contacto físico para poder comunicarse.
- **Pequeñas transacciones de datos.** Este tipo de comunicación, se realiza en base a cuatro velocidades de datos: 106, 212, 424 o 848 Kbit/s, aunque esta última no está reflejada en ISO/IEC 18092. Esta limitación se debe a que la tecnología NFC no está orientada a la transmisión masiva de datos, sino a pequeñas comunicaciones entre dispositivos.
- **Operaciones en la frecuencia ISM.** Este tipo de comunicación, se realizan en la banda de frecuencia de los 13,56 Mhz, tradicionalmente asignada a las etiquetas RFID en modo pasivo. Dicha frecuencia pertenece al conjunto de bandas de radio ISM, que son utilizadas generalmente con fines industriales, científicos y médicos (de ahí su nombre ISM, Industrial, Scientific and Medical). No se requiere licencia alguna para su uso, pero sí se debe garantizar que no se produzcan interferencias entre los dispositivos. Hecho que representa una ventaja para la implantación y uso de NFC, ya que el canal de transmisión es libre y no tiene un coste de uso asociado.

El hecho que la transmisión en NFC, se base en el concepto de pregunta y respuesta, hace que un dispositivo sólo puede responder a otro si y éste ha iniciado una comunicación con él. Para ello, cada dispositivo asume un rol diferente:

- **Iniciador.** Es el encargado de dar comienzo a la interacción. Aunque se trate de una comunicación en la que ambos dispositivos ejerzan un papel activo, el dispositivo que inaugure la comunicación será el considerado como iniciador hasta que se finalice la misma.
- **Destino.** Es el encargado de responder a la transmisión establecida por el iniciador.

De igual forma, podemos distinguir dos modos de funcionamiento:

- **Activo.** En este modo de funcionamiento, tanto el dispositivo Iniciador como el Destino generan su propio campo magnético para realizar la comunicación, por lo que ambos necesitan de una fuente de alimentación para funcionar.
- **Pasivo.** En este modo, el dispositivo Iniciador genera el campo electromagnético, y el dispositivo Destino se comunica con éste mediante la modulación de la señal recibida, es decir, obtiene la energía necesaria para funcionar del campo generado por el dispositivo Iniciador. En este caso el dispositivo Destino se encarga únicamente de establecer la

comunicación y confirmar la recepción de los datos.

En base a estas definiciones, cabe indicar que determinadas combinaciones de modos y roles no serán compatibles. Un dispositivo activo podrá actuar como iniciador o como destino en una comunicación, sin embargo un dispositivo pasivo nunca podrá ser iniciador, puesto que no puede generar su propio campo de radiofrecuencia ni emitir una señal a otro dispositivo por sí solo.

De igual forma, un dispositivo activo no podrá comunicarse con varios dispositivos pasivos a la vez aunque estos sí fuesen capaces de responder al estar bajo la influencia del campo de radiofrecuencia. El iniciador deberá seleccionar el dispositivo pasivo encargado de recibir el mensaje, siendo ignorado por el resto. En este tipo de tecnología, no están permitidos los mensajes de difusión o *broadcast*, en los que varios dispositivos reciben información de un mismo emisor.

El funcionamiento del estándar NFC también se basa en la existencia de transpondedores. Pequeños dispositivos pasivos que pueden contener fragmentos de información. Se trata de pequeñas espirales de metal a las que se les añade componentes de memoria y comunicación, que tienen un diseño completamente plano que las hace ideales para presentarse en formatos como pegatinas, tarjetas de visita, llaveros e incluso pulseras.

Los datos que contienen dichas etiquetas pueden ser de diferente tipo en base a las Definiciones de Tipos de Registros o RTD (Record Type Definition), que son formatos optimizados para la transmisión entre dispositivos NFC.

- **RTD Texto.** Es la tipología más simple, que contiene una cadena de texto en codificación Unicode. Puede utilizarse como si de texto en plano se tratara, aunque realmente se ideó para añadir metadatos de otros registros a la etiqueta.
- **RTD URI (Uniform Resource Identifie).** Esta tipología contiene una serie de datos que identifican un recurso en concreto. Dicho procedimiento de identificación será diferente en función de las informaciones almacenadas. De este modo, la etiqueta que incorpore la comunicación, permitirá remitir al usuario a un determinado recurso.
- **RTD Smart Poster.** Esta tipología engloba la mayor parte de los usos finales. Se define como una estructura que contiene los RTDs anteriores junto con acciones de control recomendadas.
- **RTD de control genérico.** Esta tipología, da acceso a funciones o aplicaciones que no puedan ser expresadas por otros RTD. Además permite enviar órdenes a otros dispositivos, pudiendo incluso seleccionar qué aplicación se desea ejecutar.
- **RTD firma.** Esta tipología, incluye en la etiqueta, como método de seguridad, una firma digital para los contenidos. Soporta firmados DSA, ECDSA y PKCS#1, que además aporta cifrado, y certificados X.509 y X9.68.

Dentro de este apartado, cabe hacer una mención especial al pago por móvil NFC. Esta aplicación es, quizá, la más publicitada y, sin embargo, la que más lentamente se está implantando.

Esto se deba, posiblemente, a la cantidad de agentes implicados en las transacciones y a la infraestructura necesaria para poner en marcha el sistema a gran escala. Dependiendo

del modo utilizado y del rol de los dispositivos, se han desarrollado varias implementaciones del pago por móvil, entre ellas, la más destacada es la cartera virtual.

Mediante la función de copia del chip NFC, el teléfono móvil se transforma en una cartera virtual, la cual contiene no sólo tarjetas bancarias, sino también cupones descuento, tarjetas de fidelización y cualquier otro documento que pueda utilizarse en una compra.

Para poder implementar esta función de forma segura, el dispositivo dispondrá de un hardware seguro llamado *Secure Element* o Elemento Seguro que será accesible por el chip NFC aun estando en modo pasivo. Éste, podrá estar integrado en la tarjeta SIM o en otros dispositivos externos.

El Elemento Seguro integrará un entorno seguro y una solución de cifrado para las aplicaciones de pago y los datos bancarios del usuario. El envío y almacenamiento de dichos datos en el teléfono será responsabilidad de la entidad conocida como Trusted Service Manager, la cuál posee las claves públicas y actúa como enlace entre los diferentes actores (banco, operador móvil y cadena comercial), facilitando el intercambio de datos entre ellos.

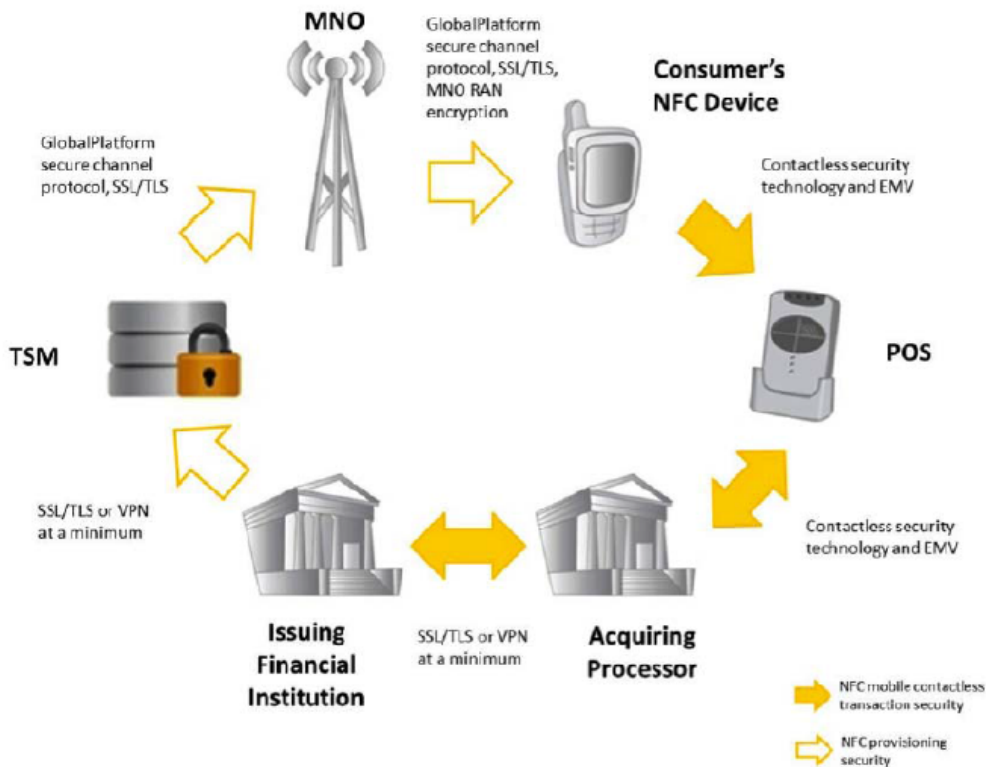
Tanto los Trusted Service Manager como el resto de entidades implicadas en el proceso de pago, conforman lo que se conoce como “modelo colaborativo”, que viene a explicar el flujo de información referente al ecosistema del modelo de pago NFC. Dicho flujo se basa en el siguiente proceso:

En primer lugar, las entidades financieras generan los datos bancarios que van a almacenarse en el Elemento Seguro del teléfono. A continuación, éstos son enviados a la TSM a través de interfaces diseñadas para la comunicación entre ambos, y se almacenan en una base de datos segura. Cuando el usuario pide la provisión del teléfono, realiza una petición al TSM a través de las redes móviles, el cual responderá facilitando los datos de pago del usuario. Una vez estos datos llegan al teléfono, son almacenados de forma cifrada en el Elemento Seguro.

Cada uno de los actores que participan en el proceso, es responsable del cifrado de la parte que gestiona. De ese modo, las entidades financieras se encargan del cifrado de datos, el TSM de las interfaces con dichas entidades y los operadores de red móvil de la securización de sus bases de datos.

Estos últimos, deben garantizar que la información no pueda ser capturada, y para ello, utilizarán conexiones fiables, tales como TLS/SSL y cifrado PKI, además del cifrado aplicado por GSM o CDMA. En la totalidad de la transmisión, se aplicarán hasta tres capas de cifrado, que supondrá la fiabilidad de la misma.

En la siguiente imagen se puede observar los diferentes elementos del ecosistema del pago con móviles NFC.



Otros actores relevantes, en el proceso, son los fabricantes de dispositivos móviles y electrónica en general, puesto que son los encargados de introducir la tecnología NFC en la sociedad, mediante la inclusión de dichas técnicas en sus productos.

2.5.4 Medidas de seguridad NFC

Debido a que la tecnología NFC se encuentra en proceso de desarrollo, no se pueden establecer unas recomendaciones precisas y concretas respecto a las medidas de seguridad del estándar NFC, pero sí se pueden definir una serie de buenas prácticas de seguridad que permitan su uso de una forma más segura. Estas buenas prácticas son:

- Mantener actualizado el sistema operativo del dispositivo y sus aplicaciones del dispositivo NFC.
- Instalar solamente aplicaciones de confianza en los dispositivos NFC.
- Leer solamente etiquetas NFC correctamente firmadas.
- Evitar cualquier acción automática por parte del sistema.
- Mantener el sistema desactivado cuando no se esté utilizando.
- Primar el cifrado en el almacenamiento de información y en las comunicaciones.
- En el caso del pago con móvil:
 - Establecer limitaciones en la cuantía de pago a partir de las cuales se requeriría autenticación.
 - Establecer las mismas limitaciones que hay marcadas para el resto de medios de pago.

Tabla resumen de las medidas de seguridad:

Medida de seguridad	Principales características
Uso de canal Seguro	<p>Se utiliza un protocolo de intercambio de llave, como por ejemplo, Diffie-Hellmann, basado en RSA, para intercambiar la clave simétrica. Con este protocolo los ataques tipo Man-in-the-Middle no son un problema.</p> <p>Se utiliza la clave simétrica para garantizar la autenticidad, integridad y confidencialidad de los datos transmitidos.</p>
Inspección de campo RF	La tecnología NFC tiene una comprobación de colisiones RF, por lo que podría llegar a detectar ataques de hombre en el medio.
Negociación de clave específica NFC	Se acuerda entre los dos dispositivos una modulación ASK 100 % que impide conocer al atacante que símbolo se está transmitiendo.
Elemento Seguro	Uso de elementos criptográficos seguros, protegidos por PIN, que realiza las funciones de cifrado y descifrado seguro a modo de HSM.

3. Seguridad de la información

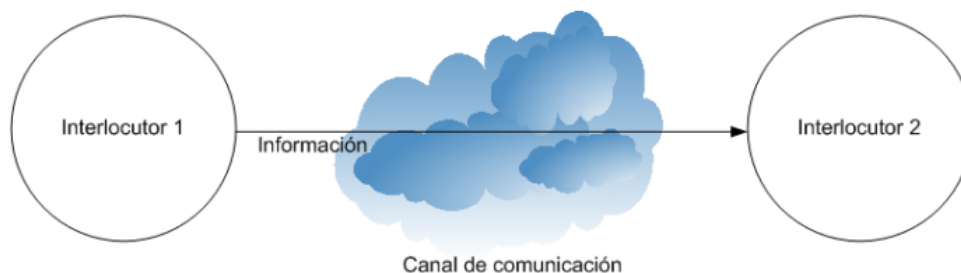
El nivel de exigencias en lo referente a seguridad de la información, ha aumentado en las últimas décadas, a causa del mayor grado de exposición de los sistemas. Antes del uso extendido de equipos de proceso de datos, la seguridad de la información se garantizaba por medios físicos y administrativos.

Actualmente, la existencia de entornos descentralizados, provoca la necesidad de transmitir datos a través de redes públicas de forma constante. Es por ello que la necesidad de seguridad también ha aumentado en base dicho crecimiento y al tipo de información en tránsito. Incluso, han surgido nuevas legislaciones con la finalidad de preservar los derechos de privacidad de las comunicaciones, como el reglamento LOPD en el caso español, la Directiva Europea 95/46/CE en la UE [7] o el Proyecto de Ley Federal [8] en EEUU.

3.1 Concepto de Seguridad de la Información

Entendemos por Seguridad de la Información, el conjunto de requisitos que es necesario llevar a cabo para preservarla. Para ilustrar estos requisitos, hay que observar el sistema como una función que transfiere información entre dos agentes.

En la siguiente imagen se puede visualizar el concepto de comunicación.



Dichos requerimientos, son la Confidencialidad, la Integridad y la Disponibilidad.

3.1.1 Confidencialidad

Entendemos por confidencialidad, la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados, permitiendo dicha disponibilidad únicamente a aquellas personas que dispongan de las debidas credenciales.

Por ejemplo, la realización de una transacción a través del aire (comunicación sin hilos) mediante tarjeta de crédito, requiere la solicitud de un número específico de dicha tarjeta, el cual será transmitido del comprador al comerciante y de éste a la red de procesamiento de transacciones.

A partir de aquí, el sistema intenta hacer valer la confidencialidad a través del cifrado del número secreto y los datos contenidos en la banda magnética, durante la transmisión de los mismos. Si durante este proceso, algún atacante consigue averiguar alguno de los

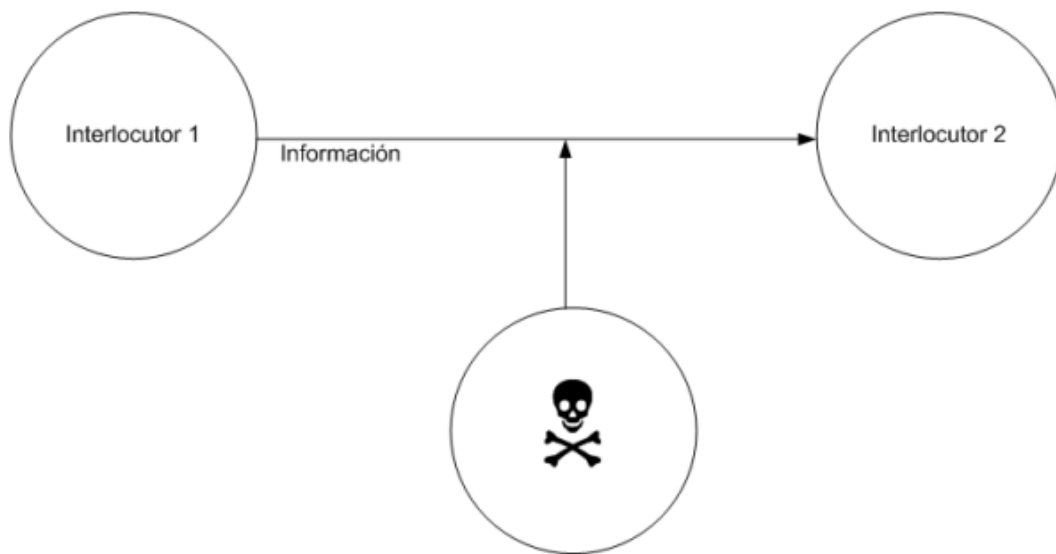
datos transmitidos, podemos decir que se ha producido una violación de la confidencialidad.

La pérdida de confidencialidad de la información puede adoptar múltiples formas: publicación de información privada, robo de un laptop con información relevante sobre una empresa, divulgación de información confidencial telefónicamente, espionaje de la pantalla del ordenador... todas ellas, acciones que constituyen una usurpación de la confidencialidad.

Exige que la información de un sistema de computadores sea accesible para lectura solamente a aquellas personas o sistemas autorizados. Este tipo de acceso incluye la visualización y otras formas de revelación, incluyendo el simple revelado de la existencia del objeto.

La amenaza a la confidencialidad se encuentra en la interceptación de la comunicación por un agente no autorizado. La probabilidad de esto ocurra dependerá del medio físico de la comunicación, o de los elementos intermedios ubicados entre los dos extremos de la comunicación.

En la siguiente imagen se puede visualizar el concepto de ataque a la confidencialidad.



3.1.2 Integridad

Entendemos por Integridad, la propiedad de mantener los datos libres de modificaciones no autorizadas. Es decir, la información debe mantenerse tal y como fue generada, sin que se produzcan manipulaciones o alteraciones por parte de personas o procesos no autorizados.

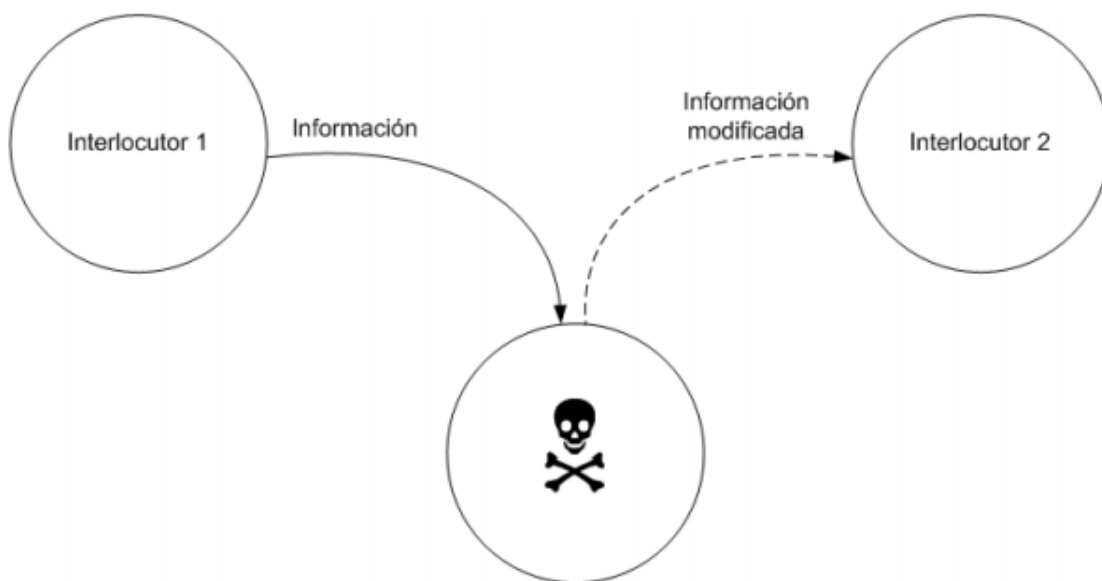
Es de vital importancia mantener inalterada una información determinada, a menos que ésta, sea modificada por personal autorizado, el cual, debe registrar dichas modificaciones, asegurando su precisión y confiabilidad. Una forma de asegurar dicha integridad, es mediante la incorporación de una firma digital, sistema que supone uno de los pilares fundamentales de la seguridad de la información.

La usurpación de la integridad, se presenta cuando una persona, programa o proceso, de modifica o elimina datos que forman parte de dicha información, ya sea de forma intencionada o accidenta.

Exige que los elementos de un sistema de computadores puedan ser modificados sólo por aquellas personas o sistemas autorizados. La modificación incluye escritura, cambio, cambio de estado, borrado y creación.

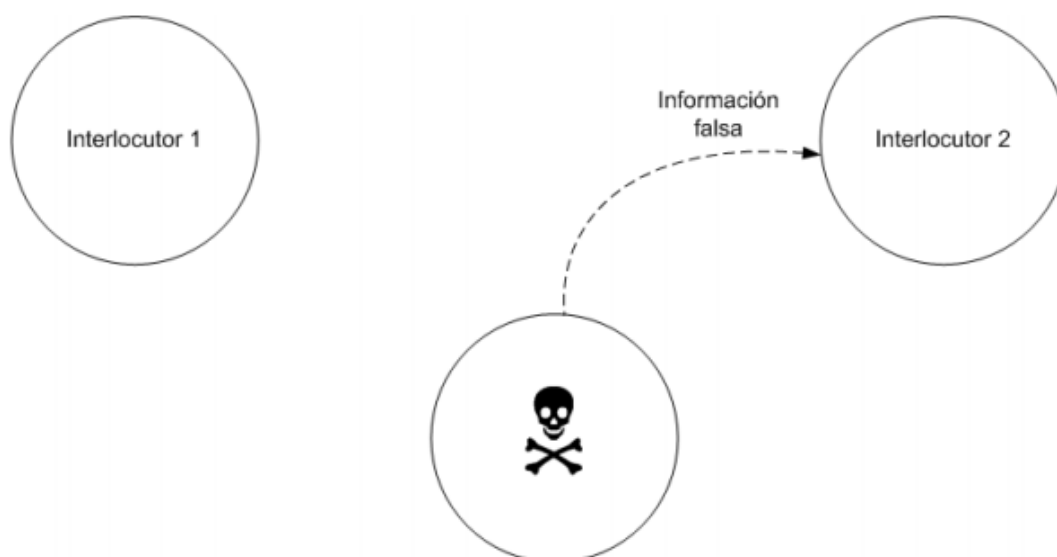
Las amenazas a la integridad vienen dadas por un acceso no autorizado y por la posibilidad de alterar la información en tránsito. Al igual que el caso de la interceptación, la probabilidad de éxito de esta amenaza dependerá de la facilidad del atacante de acceder al canal, pero sus efectos pueden ser muy perjudiciales sin no es detectado.

En la siguiente imagen se puede visualizar el concepto de ataque a la integridad



Adicionalmente, otro ataque a la integridad consiste en la inserción de información falsa en el sistema, por ejemplo retransmitiendo un paquete.

En la siguiente imagen se puede visualizar el concepto de ataque de falsificación de información.



3.1.3 Disponibilidad

Entendemos por disponibilidad, la propiedad que caracteriza la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Es decir, el acceso a los datos y a los sistemas por parte de personas autorizadas en el momento que así lo requieran.

En aquellos sistemas informáticos que se almacena y procesa información relevante, los controles de seguridad y los canales de comunicación utilizados, deben estar en continuo funcionamiento. Por eso, es muy importante evitar interrupciones del servicio ya sean debidas a cortes de energía, fallos de hardware o actualizaciones del sistema.

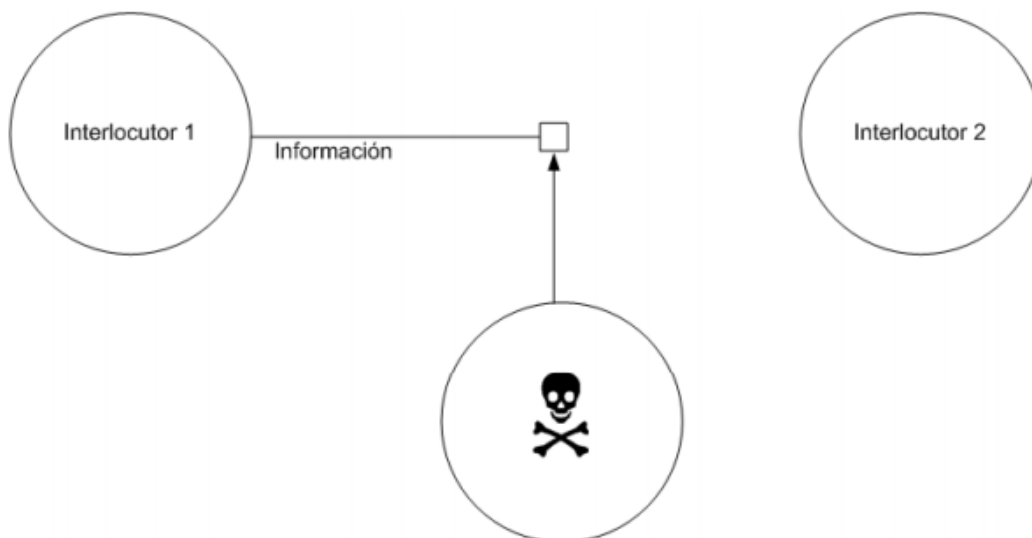
Garantizar la disponibilidad también implica la prevención de ataques de denegación de servicio. Para ello, las empresas o negocios utilizan un sistema de gestión que permite conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio.

La disponibilidad además de condicionar la integridad de la información, también permite cumplir con diferentes niveles de servicio. Para ello, se utilizan mecanismos que se implementan en infraestructura tecnológica, tales como, servidores de correo electrónico, de bases de datos, web,... y mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. Existe una gran variedad de opciones en función gama de lo que queramos proteger y el nivel de servicio que queramos proporcionar.

Exige que todos los elementos de un sistema de computadores estén disponibles a los grupos autorizados.

La amenaza a la disponibilidad se encuentra en la interrupción de las comunicaciones, ya sea interviniendo sobre el medio, sobre los interlocutores o sobre los elementos intermedios involucrados en la comunicación.

En la siguiente imagen se puede visualizar el concepto de ataque de denegación de servicio.



3.2 Clasificación de los ataques en base al proceder de los atacantes

3.2.1 Ataques pasivos

En los ataques pasivos, la interceptación de datos, el análisis del tráfico en red, la obtención de parámetros de origen y destinatario de la comunicación,... son algunos de los objetivos a conseguir por el atacante, pero la metodología utilizada en estos casos supone la no alteración de la comunicación.

El infractor tan sólo escucha y monitoriza la red, en aquellas horas donde el intercambio de datos entre las entidades relacionadas, es más habitual.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración en los datos, sin embargo, es posible evitarlos mediante el cifrado de la información.

3.2.2 Ataques activos

En los ataques activos, la obtención de datos se realiza utilizando una metodología en la que se altera la comunicación, mediante la modificación del flujo de datos transmitido o la creación de un falso flujo de datos.

Dichos ataques se pueden agrupar en cuatro categorías:

- **Usurpación / suplantación de identidad.** En ellos, el infractor, se hace pasar por su víctima, mediante la captura de secuencias y sus repeticiones, y la utilización de las mismas en operaciones en beneficio propio.
- **Retransmisión.** En ellos, el infractor captura uno o varios mensajes legítimos y los repite con la finalidad de producir un efecto no deseado. Tal como realizar una transferencia varias veces.

- **Alteración de mensajes.** En ellos, el infractor manipula, retarda o reordena el mensaje original con la finalidad de producir un efecto ilícito, tal como “Ingresa 1500 euros en la cuenta A “ modificado “Ingresa 1500 euros en la cuenta B”.
- **Degradación fraudulenta del servicio.** En ellos, el infractor inhibe el uso normal de los recursos informáticos y de comunicación en beneficio propio. De esta forma, el intruso puede denegar el servicio, paralizando temporalmente el acceso a servidores de correo, web’s, FTP,...

3.2.3 Ataques de autenticación

En los ataques de autenticación, el infractor tiene como objetivo obtener los datos de acceso de la víctima (Nombre de usuario y Contraseña) mediante el engaño y la realización de ataques de fuerza bruta o diccionario.

4. Riesgos, Amenazas y Vulnerabilidades en Redes Sin Hilos.

Las amenazas básicas que afectan a los sistemas encargados de garantizar la seguridad de la información de las redes inalámbricas, se basan principalmente en la naturaleza del medio de comunicación por el que transmiten, el aire.

Del mismo modo, al haber muchas aplicaciones referentes a estas redes, que se desarrollan en entornos no controlados e incluso hostiles, permite a los atacantes encontrar el vector de ataque adecuado.

En base a estos dos factores surgirán la mayor parte de los riesgos referentes a información e infraestructura. Por lo que las medidas de seguridad a aplicar, deberán disponer de los mecanismos necesarios para preservar los siguientes aspectos:

- Confidencialidad. Dada la fácil accesibilidad del canal de comunicación.
- Autenticidad de la información. Dado que la transmisión se realiza por el aire a todos los dispositivos ubicados en el área de influencia del emisor.
- Integridad de la información transmitida. Dada la relevancia de evitar posibles modificaciones accidentales o malintencionadas.
- Vigencia de la información. Dada la importancia de evitar la retransmisión de información obsoleta.
- Disponibilidad del canal y los dispositivos. Dada la relevancia de evitar ataques de denegación de servicio.
- Acceso lógico a la red. Dada la necesidad que éste sea exclusivo para los nodos designados.
- Captura de algún nodo. Dada la necesidad que la entrada física al mismo no permita obtener la información de acceso que contiene.
- Prevención de la suplantación de los nodos por dispositivos malintencionados. Dado que éstos, pueden dañar la integridad mediante la inyección de información falsa o a la disponibilidad de la red.

4.1 Ataques sobre la pérdida de confidencialidad

En base a la confidencialidad de los datos transmitidos, pasamos a describir varios ataques que se producen de forma generalizada en todas las comunicaciones sin hilos:

4.1.1 Interceptación o Sniffing / Eavesdropping.

Dicho ataque, también conocido como **passive wiretapping** ([CES91]) consiste en la captación de información confidencial (en claro o cifrada) por parte de un atacante, de forma fraudulenta.

Aunque en un principio, dicho ataque es completamente pasivo, la peligrosidad del mismo, reside en el hecho, que es muy difícil de detectar mientras se produce. De forma que un intruso, puede capturar información privilegiada y claves para acceder a más datos, sin que nadie se dé cuenta hasta que dicho ataque se convierta en activo mediante la utilización de la información capturada por parte del atacante.

Este ataque, conocido como **sniffing**, utiliza como medio para interceptar la información, la captura de tramas que circulan por la red. Para ello, utiliza un programa que se ejecuta en una máquina conectada a la red o un dispositivo que se engancha directamente al cableado.

Estos dispositivos, se denominan **sniffers** de alta impedancia y se conectan en paralelo con el cable, de forma que la impedancia del cable y el aparato, es similar a la del cable solo, dificultando enormemente su detección.

Para combatir estos ataques, encontramos varias soluciones:

La más barata a nivel físico es no permitir la existencia de segmentos de red de fácil acceso que se conviertan en el lugar idóneo para que un atacante conecte uno de estos aparatos y capture todo nuestro tráfico. No obstante, esto resulta difícil en redes ya instaladas, donde no se puede modificar la arquitectura de la misma.

Es aconsejable analizar regularmente nuestra red para verificar que todas las máquinas activas, tienen acceso autorizado, puesto que las tomas de red libre, pueden ser usurpadas por un atacante que conecte su portátil y capture el tráfico que circule por allí.

Otra posible solución, generalmente gratuita pero que poco tiene que ver con el nivel físico, sería el uso de aplicaciones de cifrado para realizar las comunicaciones o el almacenamiento de la información (hablaremos más adelante de alguna de ellas).

La aplicación de este mismo remedio a nivel físico, sería el uso de dispositivos de cifra (no simples programas, sino hardware) tales como chips que implementan algoritmos como DES. Dicha solución es muy poco utilizada en entornos de I+D, puesto que es mucho más cara que la utilización de implementaciones software de tales algoritmos, y además, en muchas ocasiones tan sólo se diferencian de éstos, en la velocidad.

Otra posible respuesta a éste ataque, cuyo coste es más elevado, sería la utilización de cableado en vacío. Esta acción consiste en situar los cables en tubos donde artificialmente se crea el vacío o se inyecta aire a presión. De este modo, si un atacante intenta “pinchar” el cable para interceptar los datos, se rompe el vacío o el nivel de presión y el ataque es detectado de forma inmediata. Dicha solución sólo se aplica en redes de perímetro reducido para entornos de alta seguridad, dado su coste económico.

Antes de finalizar este punto, debemos mencionar un peligro que en muchas ocasiones no se tiene en cuenta; la interceptación de datos emitidos en forma de sonido o simple ruido en nuestro entorno de operaciones.

Imaginemos una situación en la que los responsables de seguridad de una empresa, se reúnan para tratar nuevos mecanismos de protección; toda la información que en esa reunión se hable puede ser captada por múltiples metodologías, algunas de las cuales son tan simples que ni siquiera se contemplan en los planes de seguridad. Una simple tarjeta de sonido instalada en un PC ubicado en la sala, un teléfono mal colgado... puede proporcionar al atacante información de gran utilidad para enemigos potenciales.

Para evitar dichas intromisiones, existen múltiples soluciones, en ocasiones, tan sencillas como en el caso de los teléfonos fijos, comprobar que están bien colgados o incluso desconectados de la red telefónica.

El caso de los móviles suele ser más complicado de controlar, ya que su pequeño tamaño permite camuflarlos fácilmente; No obstante, podemos instalar en la sala donde se lleve a cabo la reunión, un sistema de aislamiento que bloquee el uso de dichos teléfonos. Se trata de un mecanismo que ya está siendo utilizado en entornos tales como teatros, salas de conciertos... para evitar posibles ruidos mediante el bloqueo de cualquier transmisión en los rangos de frecuencias en los que trabajan los diferentes operadores telefónicos.

Otra medida preventiva, para la fuga de datos ya no por voz, sino vía ruido ambiente, sería la sustitución de teléfonos fijos de disco, por teléfonos de teclado, puesto que el ruido de un disco al girar puede permitir a un atacante deducir el número de teléfono marcado desde ese aparato.

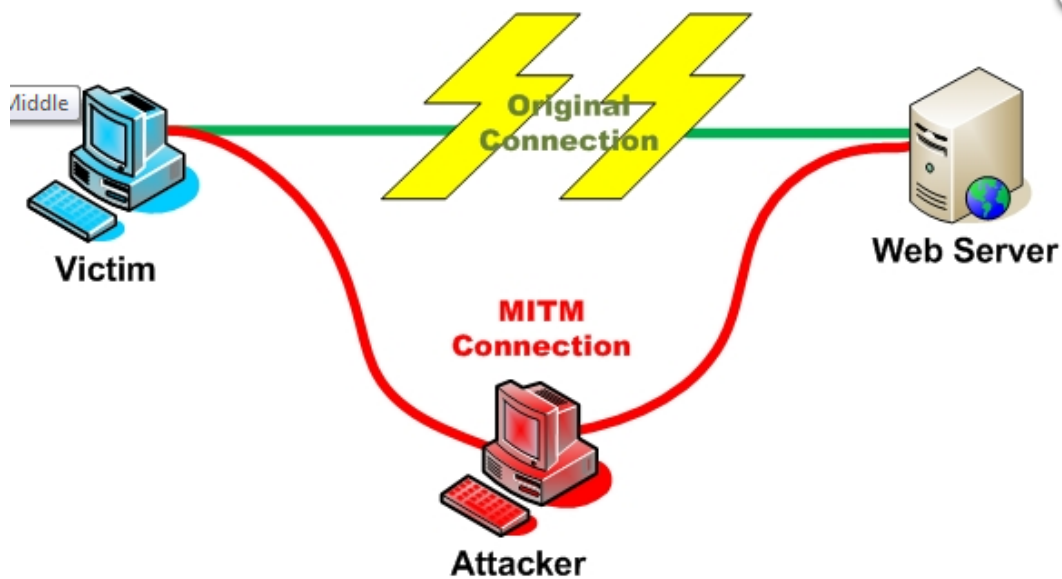
4.1.2 Ataques “Man in the Middle” o de intermediario.

Dicho ataque, consiste en el hecho que un infractor se haga con el control de lectura, emisión y modificación de mensajes producidos en un canal entre 2 máquinas, sin que ninguna de ellas conozca dicha situación.

Un usuario con malas intenciones, se coloca entre el sistema 1 y el sistema 2 y todo aquel tráfico enviado de un sistema a otro, pasará en primer lugar por él, de modo que éste, puede realizar modificaciones de los mismos a voluntad.

En la siguiente imagen se aprecia el desvío de información que se produce entre el sistema 1 y el 2.

En la siguiente imagen se puede visualizar el concepto de ataque de Man in the Middle.



En un ataque MitM la comunicación no sólo es interceptada por el atacante, como ocurre en el caso del eavesdropping, sino que además ésta, pasa a través de él. Los sistemas emisor y receptor creen estar comunicándose directamente cuando en realidad lo están haciendo a través del atacante, que aprovecha esta situación para manipular la información que se intercambian.

4.2 Ataques sobre la pérdida de Integridad

En base a la integridad de los datos transmitidos, pasamos a describir varios ataques que se producen de forma generalizada en todas las comunicaciones sin hilos:

4.2.1 Corrupción de datos

Dicho ataque hace referencia a la introducción de cambios no deseados en una información determinada, durante la transmisión o recuperación de la misma. Los equipos de almacenamiento y los sistemas de transmisión, proporcionan medidas para garantizar la integridad de la información.

La corrupción de los datos durante la transmisión de los mismos, se puede deber a causas medioambientales, especialmente si se utilizan métodos de transmisión inalámbricos.

La pérdida de datos durante el almacenamiento de los mismos, se puede deber a aspectos de hardware y software defectuoso. Accidentes generales y de desgaste de los medios de comunicación se englobarían en el primero, mientras que errores en el código, pertenecerían al segundo.

La corrupción de los datos, en general, puede ser detectado por el uso de sumas de verificación y puede ser corregido mediante el uso de códigos de corrección de error.

Si un dato que no debe ser modificado, ha sufrido alguna alteración, mediante la aplicación de procedimientos como la retransmisión automática o la restauración de copias de seguridad, pueden ser subsanados.

Ciertos niveles de arreglos de RAID tienen la capacidad de almacenar y evaluar los bits de paridad de datos a través de una serie de discos duros, permitiendo la reconstrucción de aquellos que se encuentren dañados, mediante un único o múltiple disco, en función del nivel de RAID aplicado.

Si utilizamos los mecanismos adecuados para detectar y remediar la corrupción de datos, la integridad de los mismos, se puede mantener. Esto es especialmente importante en la banca, donde un error puede afectar drásticamente datos tan relevantes como el saldo de una cuenta. Y también en el uso de cifrado o compresión de datos, puesto que un pequeño error, puede hacer inservible una amplia base de datos.

4.2.2 Modificación de datos.

Dicho ataque hace referencia a la modificación desautorizada de los datos o el software instalado en el sistema víctima, incluyendo el borrado de archivos.

Es particularmente serio cuando el infractor que los realiza obtiene derechos de Administrador o Supervisor, disponiendo, entonces, de la capacidad de disparar cualquier comando y alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. En estos casos, el Administrador legítimo del sistema, requerirá darlo de baja durante horas o días hasta la total restauración de la información modificada o eliminada.

Al igual que otros ataques, éste puede ser llevado a cabo por Insiders u Outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor. Son innumerables los casos de este tipo: empleados bancarios o externos que crean falsas cuentas para derivar fondos de otras cuentas, contribuyentes que pagan para que se les elimine una deuda impositiva...

Múltiples Web Sites han sido víctimas de este ataque mediante el cambio de imágenes originales por otras de índole terrorista o de humor. Un ejemplo de esto, es el ataque de The Mentor a la NASA, o la reciente modificación del Web Site de la BBC en febrero de este mismo año.

En otras ocasiones, se produce el reemplazo de versiones de software, por otras con igual denominación, pero que incorporan código malicioso (virus, troyanos...) La utilización de dichos programas estaría dentro de esta categoría, pero se profundizará en ellos en otro apartado.

4.3 Pérdida de Disponibilidad

En base a la disponibilidad de los datos transmitidos, pasamos a describir el principal ataque que se producen de forma generalizada en todas las comunicaciones sin hilos:

4.3.1 Denegación de servicio.

Dicho ataque hace referencia al conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo, con la finalidad que los usuarios legítimos del sistema no puedan acceder a los servicios prestados por el mismo.

El ataque consiste en provocar la saturación del servidor mediante el envío continuo de peticiones de servicio, hasta que éste no puede atenderlas y se colapsa.

Un método más sofisticado es el llamado Ataque de Denegación de Servicio Distribuido (DDoS) mediante el cual se envían peticiones de forma coordinada entre varios equipos, ante el desconocimiento de los Administradores legítimos del equipo. Esta técnica, se lleva a cabo mediante la utilización de programas malware que permiten la toma de control remoto del equipo.

4.4 Resumen

En base a lo expuesto en los apartados anteriores, la siguiente tabla describe de forma resumida los diferentes ataques que afectan a cada una de las tecnologías sin hilos analizadas:

	Confidencialidad		Integridad			Disponibilidad
	Sniffing	“Man in the Middle”	Corrupción	Modificación	Inserción	DoS
WIFI(802.11)	Afectado	Afectado	Afectado	Afectado	Afectado	Afectado
Bluetooth	Afectado	Afectado	Afectado	Afectado	Afectado	Afectado
RFID	Afectado	Afectado	Afectado	Afectado	Afectado	Afectado
NFC	Afectado	No Afectado	Afectado	Afectado	Afectado	Afectado

5. Ataques específicos a tecnologías sin hilos

5.1 Ataques a la tecnología 802.11

5.1.1 Ataques para acceso al medio

5.1.1.1 Ataque a la autenticación mediante claves WEP

El protocolo WEP se basa en el requerimiento de una clave secreta y compartida por las estaciones y el AP para dar comienzo a la comunicación.

Dicha clave, supone una de las principales carencias del sistema, dado que éstas, deben ser comunicadas a los clientes por una vía alternativa y en función del número de éstos, puede resultar un acometido muy costoso que suponga, en muchos casos, poca frecuencia en la modificación de las mismas.

El modo de funcionamiento, consiste en la petición inicial de asociación al AP, realizada por parte de una máquina a un punto de acceso que utilice WEP, el cual a su vez, responderá con un texto aleatorio (desafío). El cliente deberá cifrar dicho texto con su clave compartida y enviar la respuesta al AP, el cual, descifrará el texto y comparará su propia clave con la enviada, permitiendo o no, el acceso al cliente.

El algoritmo utilizado en el cifrado de la comunicación WEP se conoce como RC4. Dicho algoritmo, conforma una parte de la clave compartida, que se mantiene constante en todo momento. La otra parte de la clave es dinámica y cambia en cada trama con el objetivo de impedir que un atacante pueda recolectar datos suficientes como para

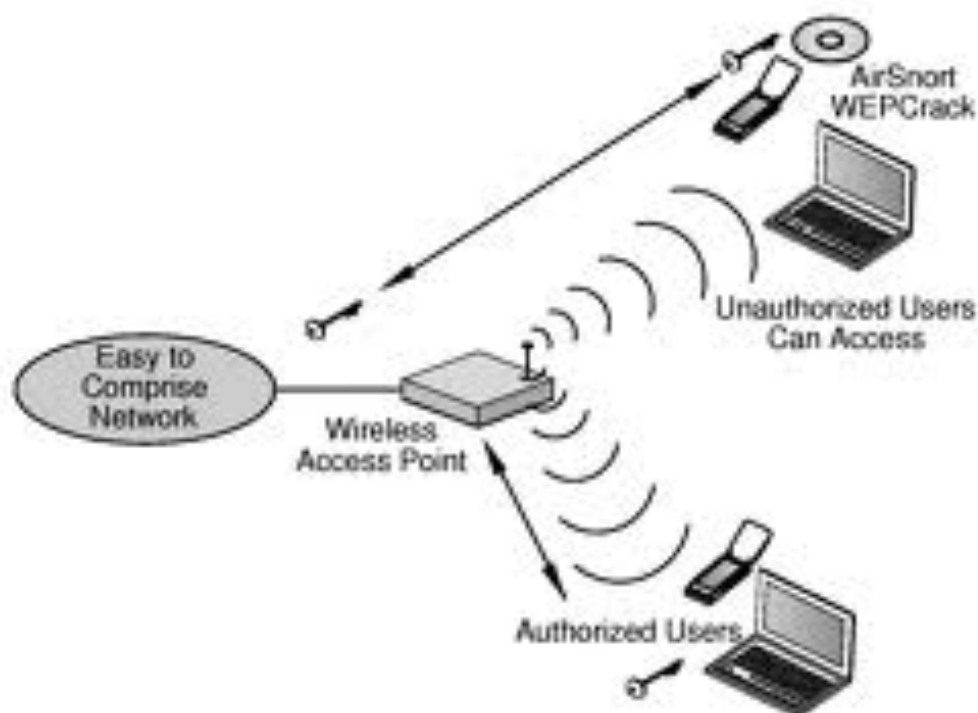
averiguarla. A esta parte se la conoce como IV (vector de inicialización) y según el estándar debe ser modificada en el envío de cada paquete. Es decir, la clave final asignada para el cifrado/descifrado será la vinculación del IV y la clave compartida.

El tamaño del vector de inicialización es de 24 bits, por lo que el de la clave secreta será de 40 bits (en claves de 64bits) o de 104 bits (en claves de 128bits). Este aspecto, puede suponer malentendidos en cuanto al por qué de si la clave es de 128bits sólo se pueden escribir 13 caracteres ($13 \cdot 8 = 104$) y no 16 ($16 \cdot 8 = 128$) como cabría esperar.

Dicho vector, únicamente lo conoce uno de los extremos, por lo que será necesario enviarlo sin cifrar al otro, para que éste pueda reconstruir la clave secreta e iniciar el proceso de descifrado de datos.

En este proceso, un atacante que explote correctamente ciertas debilidades del mismo, puede llegar a comprometerlo. Únicamente debe extraer un volumen de paquetes IV que le permita, mediante un proceso de “cracking”, obtener la clave WEP. A partir de aquí, la captura de datos la realizará mediante una gran variedad de técnicas, tales como la des autenticación de los clientes, inyección de tráfico, mac spoofing,...

En la siguiente imagen se muestra el esquema del ataque.



5.1.1.2 Ataques a la autenticación mediante claves WPA/WPA2

El protocolo WPA surge como solución temporal, en referencia a la seguridad de las redes Wireless, dada la debilidad del protocolo WEP.

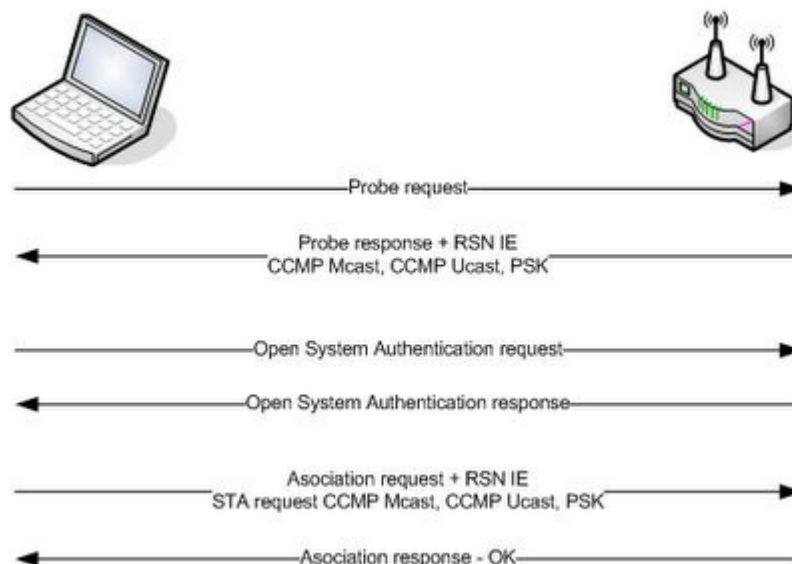
En el momento en que el estándar 802.11i sale a la luz, la WIFI Alliance proporciona el protocolo WPA2 a todos aquellos dispositivos que cumplen con las especificaciones marcadas por el nuevo estándar.

Tanto la WPA como la WPA2 soportan el protocolo 802.1x para la autenticación en ámbitos empresariales y domésticos. Su principal diferencia, reside en el algoritmo de cifrado que utilizan. Mientras que el WPA emplea el algoritmo TKIP (Temporary Key Integrity Protocol), fundamentado en el RC4, la WPA2 utiliza el CCMP (Counter-mode/CBC-MAC Protocol) fundamentado en AES (Advanced Encryption System).

Otro punto en el que difieren ambos protocolos, es en el algoritmo utilizado para el control de la integridad del mensaje. Mientras WPA utiliza una versión poco elaborada para la generación del código MIC (Message Integrity Code), WPA2 implementa una versión mejorada del mismo.

El modo de funcionamiento, de igual modo que en el protocolo WEP, consiste en la petición de autenticación que podrá ser abierta o con clave compartida y una segunda fase de asociación. En aquellos casos en los que el punto de acceso no esté emitiendo, se produce una Fase de Prueba inicial, en la que el cliente envía el ESSID de la red wireless a la que quiere conectarse, esperando que el punto de acceso responda y así iniciar las fases de Autenticación y Asociación.

En la siguiente imagen se puede observar el proceso de autenticación de WPA



Los protocolos WPA y WPA2, tienen pequeñas debilidades que pueden ser explotadas por atacantes, pero ninguna de ellas supone un elevado grado de peligrosidad si se aplican unos mínimos requerimientos de seguridad.

La vulnerabilidad más destacada de estos protocolos, es el ataque contra la clave PSK de WPA/WPA2, basado en el hecho que el cliente inicia la conexión a la red sin iniciar el proceso de autenticación WPA / WPA2, por lo que el tráfico enviado no está cifrado. Este hecho, puede ser aprovechado por un atacante que mediante el envío de una trama de des-asociación al cliente, podría provocar que éste se desasocie y tenga que volver a iniciar el proceso. Esto se conoce como ataque 0 o de des-asociación.

Un atacante que quiera quebrantar una red WPA2-PSK, tratará de capturar el intercambio de números que se produce entre cliente y AP, para de ese modo, junto con el ESSID y las direcciones MAC del cliente y el punto de acceso, obtener la clave compartida utilizada y así poder conectarse a la red.

5.1.1.3 Ataques a la autenticación EAP, EAP-MD5, LEAP, EAP-TTLS, PEAP, EAP-FAST.

El protocolo Extensible Authentication Protocol y todas sus variables basan la autenticación en contraseñas asimétricas, excepto el EAP-FAST que lo hace en base a claves simétricas.

En el caso concreto del EAP-FAST, la autenticación del servidor es del tipo “Diffie-Hellman”, que establece claves entre partes que no han tenido contacto previo, utilizando un canal inseguro y de una forma anónima. Hecho que implica que no se pueda verificar quién se encuentra en el otro extremo.

Todo ello, supone que dichos protocolos sean susceptibles de ataques de diccionario / fuerza bruta. Un atacante, mediante la realización de un MITM, puede hacerse pasar por el punto de acceso y el servidor de autenticación y esperar a que un usuario se conecte y facilite el usuario en claro y las contraseñas con el algoritmo hash, capturando la sesión MS-CHAP para luego crackearlo con ASLEAP.

5.1.1.4 Fuerza Bruta

Este tipo de ataque consiste en la obtención de claves mediante la introducción de todas las combinaciones posibles, hasta dar con aquella que permite el acceso.

Esta metodología, tiene como limitación principal, la cantidad de tiempo que se emplea hasta obtener la cifra secreta, teniendo en cuenta la velocidad de procesamiento de una computadora.

Por todo ello, es conveniente utilizar claves complejas y largas que dificulten la aplicación de dichas metodologías de fuerza bruta.

Actualmente, el uso creciente de las GPU (Graphics Processing Units) está provocando que dichos ataques se estén convirtiendo en algo sencillo y efectivo de realizar.

5.1.1.5 Ataques de Fuerza Bruta usando GPUs

El aumento en la potencia de las GPUs, permite realizar un gran número de operaciones por segundo, hecho que facilita la realización de este tipo de ataques. Según la información que manejan los expertos, la ruptura de claves se realiza de una forma 10.000 veces más rápida que si se utilizara una CPU convencional.

La mejor manera de evitar este tipo de ataques es dotando a la conectividad inalámbrica de doble autenticación bajo VPN. Mediante este formato, se emplea un “token” como segundo factor de autorización de acceso y se confía el tráfico a una red virtual privada.

Como herramientas para llevar a cabo este tipo de ataques, cabe destacar CUDA y ElcomSoft, entre otras.

En el primer caso, la configuración de múltiples tarjetas gráficas de gran capacidad en máquinas convencionales, junto con la utilización del lenguaje CUDA, han supuesto un incremento considerable en la potencia de cálculo.

En el segundo, la aplicación Distributed Password Recovery, utiliza la GPU para obtener contraseñas que protegen diferentes tipos de documentos, tales como pdf, zip,... e incluso contraseñas Windows.

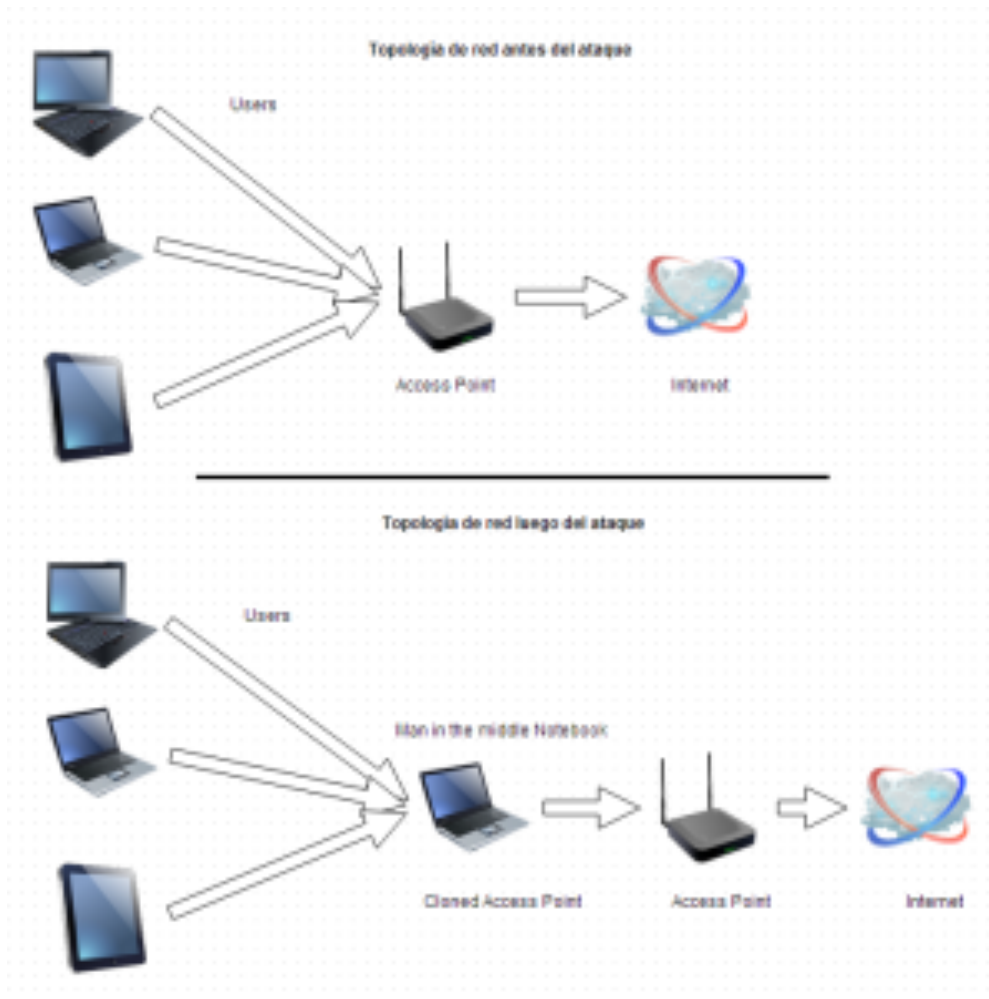
5.1.2 Falsificación de identidad

5.1.3 Rogue Access Points

Este tipo de ataque consiste en la suplantación del punto de acceso. El objetivo, es conseguir que la víctima se conecte al equipo del atacante, que realiza funciones de punto de acceso legítimo, y a partir de aquí, éste se encargará de redirigir el tráfico en beneficio propio.

Se considera una forma sencilla de realizar un ataque Man In The Middel, puesto que el atacante podrá realizar funciones de AP e interceptar la totalidad de las comunicaciones. De igual modo, podrá realizar ataques tipo DoS y usurpar datos de clientes que se encuentren conectados o incluso monitorizar las actividades de los mismos.

En la siguiente imagen se muestra el esquema del ataque.



Este ataque puede llevarse a cabo con un AP modificado o con un portátil, siempre y cuando disponga de las aplicaciones necesarias, tales como http, DNS, DHCP y un Portal Cautivo para re direccionar el tráfico.

Un factor decisivo en el éxito del ataque es la suplantación del AP legítimo por otro de iguales características, recreado en el Rogue AP . Para ello, se debe copiar el BSSID, ESSID, las configuraciones de seguridad de la red y la clave.

La técnica del Rogue Access Point también puede ser utilizada para realizar los ataques de MiMT descritos en el apartado 5.6 de este mismo documento.

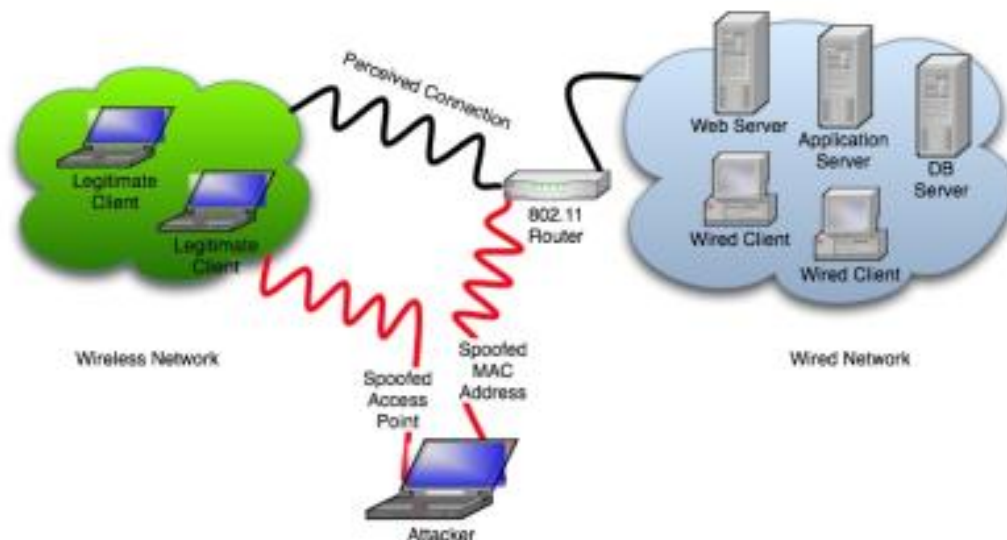
5.1.4 El robo de información vía redes Wi-Fi (Wi-phishing)

Este tipo de ataque consiste en aprovechar las debilidades que ofrecen las redes WIFI públicas para capturar contraseñas, números de tarjetas de crédito e incluso comunicaciones que pudieran estar cifradas, mediante lo que se conoce como Wi-phishing.

Dichas redes, ofrecen acceso compartido a Internet a múltiples usuarios, por lo que cualquier persona con un dispositivo inalámbrico dentro del alcance del punto de acceso, puede conectarse a la red y utilizar Internet.

Los propietarios de los establecimientos para facilitar el uso de este sistema a sus clientes, minimizan los requisitos de acceso, evitando de ese modo, problemas de compatibilidad entre dispositivos y sistemas operativos. Para ello, suelen deshabilitar gran parte de las medidas de seguridad provocando que la información privada de dichos usuarios se transmita sin protección por la Web.

En la siguiente imagen se muestra el esquema del ataque.



5.1.5 MAC Address Spoofing

Este tipo de ataque consiste simplemente en detectar una MAC que esté enviando tráfico y suplantarla.

Dicha metodología se aplica en redes WIFI conocidas como portales captivos, donde la utilización de la misma, junto con la Sesión Hijacking (robo de sesión) da como resultado la obtención de acceso.

5.1.6 Vulnerabilidad Hole 196

Este tipo de ataque consiste en el envío de un mensaje con una clave GTK a una MAC dirigida, para que, de ese modo, la víctima procese el paquete broadcast y salvo que la tabla de ARPs tenga la resolución de la MAC del Gateway estática, se produzca el envenenamiento de la IP que permita la suplantación del router.

A partir de aquí, cuando la víctima se comunice con el Gateway, se aplicarán las claves PTK asociadas a esa IP, que el atacante entregará para realizar el MITM.

En ningún momento se rompe el sistema de autenticación de WPA / WPA-2 Enterprise, sino que el acceso fraudulento se realiza de forma oculta, de modo que hasta que no aparezcan soluciones IDS que inspeccionen todo el tráfico que vaya cifrado con claves GTK, el ataque no será descubierto.

Dicho ataque fue descubierto en 2010 por Airtight Networks y se lo denominó Hole 196 en referencia a la página del estándar IEEE 802.11 que hace referencia a los mensajes enviados con claves de grupo, las cuales carecen de protección contra Spoofing. Con lo que cualquiera con acceso autorizado a la red WIFI puede descifrar y robar información confidencial de cualquier otro que se encuentre conectado a la misma red inalámbrica, inyectar tráfico malicioso o comprometer dispositivos autorizados.

5.2 Ataques a la tecnología Bluetooth

Los ataques a la tecnología Bluetooth, se realizan básicamente a teléfonos móviles. Este paralelismo se debe en gran medida a que en la actualidad, existen muy pocos terminales móviles que no posean implementada esta tecnología, y en ocasiones presentan mecanismos de seguridad muy rudimentarios.

Actualmente los terminales móviles se han convertido en una herramienta esencial de la vida moderna, siendo habitual que las personas utilicen dichos dispositivos para multitud de funciones, tales como:

- Obtención de información constante y actualizada.
- Realización de transacciones financieras.
- Pago de servicios.
- Almacenamiento de datos.
 - Datos personales y financieros.
 - Datos laborales.
- Diversión y entretenimiento.

Debido al uso generalizado y al incremento del número de terminales, y dadas las limitaciones de los mecanismos de protección y seguridad que actualmente poseen. Los teléfonos móviles, se han convertido en un foco de ataques, tanto para usuarios personales como corporativos y uno de los vectores utilizados, será la implementación del protocolo bluetooth.

5.2.1 Ataques a implementación de Bluetooth en terminales móviles.

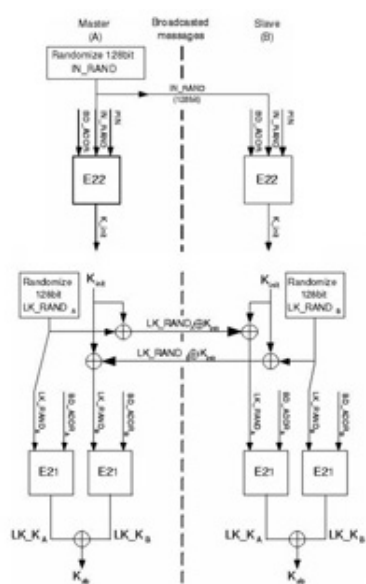
5.2.1.1 Bluetooth Pin-cracking

Este tipo de ataque se basa en el proceso de emparejamiento de los dispositivos de dicha tecnología. El objetivo es que dos dispositivos Bluetooth se puedan comunicar si hay una relación de confianza entre ellos.

Para que dos dispositivos puedan comunicarse por primera vez, deben llevar a cabo un proceso denominado “emparejamiento”, mediante el cual, se crea una clave de enlace común de una forma segura. Este procedimiento requiere que el usuario de cada dispositivo introduzca un código de seguridad Bluetooth (código PIN, Personal Identification Number) de hasta 16 bytes de longitud que debe ser el mismo en los dos terminales.

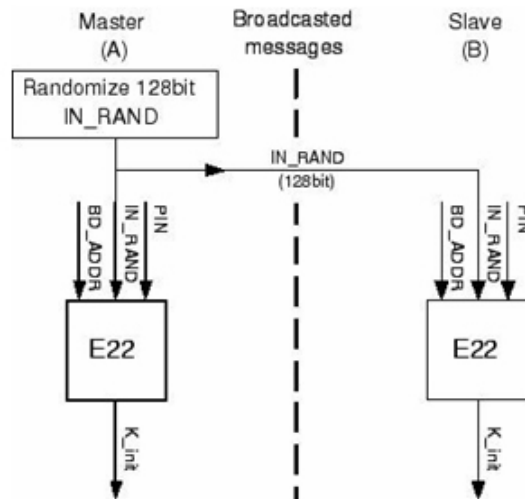
En la siguiente imagen se muestra el esquema de asociación bluetooth.

The screenshot shows a mobile phone interface with a Bluetooth connection prompt. The prompt asks: "Sony Ericsson z750 desea conectarse con el dispositivo utilizando Bluetooth. ¿Desea agregar Sony Ericsson z750 a la lista del dispositivo?". Below the prompt is a keyboard with various symbols and numbers. The phone's status bar at the top shows "Inicio", "14/02/09", and "16:09".



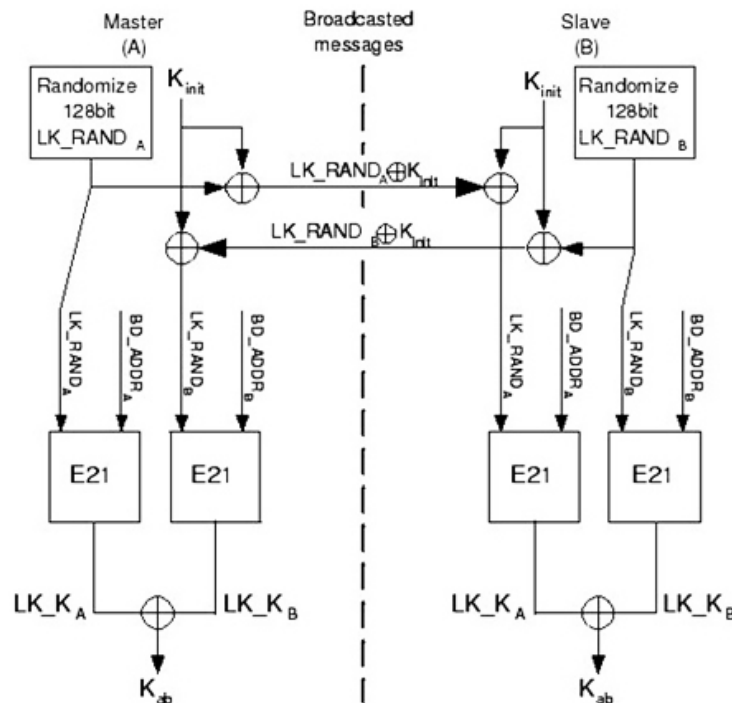
A partir del código PIN, se obtiene la clave de enlace común a través del siguiente algoritmo:

1. Se genera una clave de inicialización común Kinit de 128 bits usando el algoritmo E22 a partir del código de seguridad Bluetooth (PIN), la longitud del mismo, la dirección BD_ADDR de 48 bits y un número aleatorio IN_RAND.



- Se genera la clave de enlace K_{ab} usando el algoritmo E21. Los dispositivos utilizan la clave de inicialización K_{init} para intercambiar dos nuevos números aleatorios, conocidos como LK_RAND_A y LK_RAND_B . Cada dispositivo genera uno de estos números y se lo envía al otro terminal de forma XORada bit a bit con K_{init} .

Dado que ambos dispositivos conocen K_{init} , de igual forma conocen LK_RAND . A partir de la dirección BD_ADDR y LK_RAND , se genera la clave de enlace K_{ab} .



- Una vez que los dispositivos emparejados disponen de la clave de enlace K_{ab} , ésta, se utiliza para autenticarse automáticamente en las sucesivas conexiones.

Si un atacante, mediante la técnica de sniffing consigue averiguar el emparejamiento de dos dispositivos Bluetooth, puede llegar a crackear el algoritmo de emparejamiento de los mismos, por fuerza bruta.

En 2005 Yaniv Shaked y Avishai Wool publicaron “Cracking the Bluetooth PIN”, un procedimiento criptológico teórico para crackear el algoritmo de emparejamiento Bluetooth. Básicamente, consistía en ir probando entradas por fuerza bruta hasta que las claves temporales generadas durante el desarrollo del algoritmo coincidan con aquellas que se habían capturado mediante la técnica de sniffing aplicada a los dos dispositivos.

Para ello, se requieren los siguientes requerimientos de entrada del algoritmo:

- **Código PIN.** El cual se va generando por fuerza bruta (suelen ser de 4 dígitos).
- **Direcciones BD_ADDR de los dispositivos emparejados.** Las cuales se obtienen realizando una consulta `hci_inquiry`.
- **Número aleatorio IN_RANDOM.** El cual, en realidad resulta no ser tan aleatorio, puesto que depende, en cierta manera, de un date/time stamp que se puede obtener a partir del clock-offset.

A lo largo del desarrollo del algoritmo de emparejamiento, los dispositivos participantes se intercambian ciertas claves temporales, que un atacante puede capturar si es capaz de sniffar el tráfico de la piconet a la que pertenecen dichos dispositivos. Comparando dichas claves temporales con las obtenidas crackeando el algoritmo por fuerza bruta se puede llegar a obtener el PIN y la clave de enlace que comparten los dispositivos emparejados.

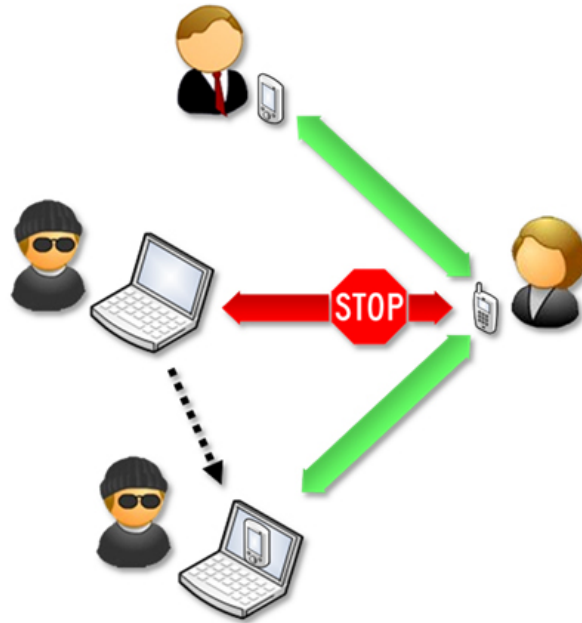
En 2006, Thierry Zoller elabora una herramienta para Windows, denominada BTCrack, que permite crackear por fuerza bruta la clave de enlace, en base a las claves temporales capturadas sniffando el emparejamiento de dos dispositivos Bluetooth.

Dicha herramienta irá evolucionando durante los años siguientes, en base a disminuir los tiempos de respuesta y liberar el código fuente de la versión OSS de BTCrack para Linux.

5.2.1.2 Ataque BD_ADDR spoofing

Este tipo de ataque consiste en la suplantación de la identidad de un dispositivo, del que se ha obtenido la clave de enlace bluetooth y utilizar sus credenciales para acceder a perfiles que requieran autorización y autenticación con el fin de atacar otro terminal Bluetooth.

En la siguiente imagen se muestra el esquema del ataque.



El BD_ADDR spoofing es similar al clásico ataque MAC Spoofing en redes Ethernet. Éste, permite a un atacante suplantar la dirección MAC de un equipo para reemplazar su identidad y llevar a cabo acciones maliciosas contra el resto de equipos de la red, ya sea interceptando comunicaciones dirigidas al equipo usurpado o utilizando sus credenciales con el fin de acceder a un sistema de acceso restringido.

Dado que hay dos mecanismos de seguridad en Bluetooth, el ataque BD_ADDR Spoofing se puede desarrollar en dos niveles:

- Suplantación de la dirección BD_ADDR de un dispositivo de confianza para acceder a perfiles que requieren autorización.
- Suplantación de la dirección BD_ADDR y obtención de la clave de enlace generada durante el emparejamiento para acceder a perfiles que requieren autenticación.

5.2.1.3 Ataque Bluesnarf

Este tipo de ataque consiste en la extracción de archivos de un teléfono móvil Bluetooth a través del Perfil de Carga de Objetos (OBEX Object Push) sin la correspondiente autorización del propietario.

Esto se debe a la incorrecta implementación del Perfil de Carga de Objetos en los antiguos terminales móviles, que carecían de mecanismos de autenticación, permitiendo la descargar, mediante una operación OBEX GET, de archivos con nombre conocido, tales como la agenda de contactos almacenada en el terminal en telecom/pb.vcf o el calendario de citas almacenado en telecom/cal.vs.

En la actualidad, la mayoría de teléfonos móviles Bluetooth incorporan mecanismos de autorización en el acceso al Perfil de Carga de Objetos (OBEX Object Push), pero ésta puede ser usurpada mediante las distintas técnicas analizadas con anterioridad.

El Perfil de Carga de Objetos (OPUSH u OPP, Object Push Profile) establece los requisitos a tener en cuenta, a la hora de implementar el modelo de uso de carga de objetos, basado en el protocolo OBEX Object Push, el cual, se encarga de llevar a cabo esta tarea entre dispositivos Bluetooth.

La funcionalidad inicial de dicho Perfil de Carga, consistía en llevar a cabo la carga y descarga de citas (vCalendar) y el intercambio de tarjetas de visita (vCard) entre dispositivos Bluetooth. Actualmente, el perfil conserva esta labor, pero también se utiliza para realizar transferencias de archivos.

Especificación IrMC de los archivos OBEX:

Filename	Description	Supported operations
Device Info		
telecom/devinfo.txt	Information hardware version, software version, serial number, etc. Character sets	GET
telecom/rtc.txt	The Real Time Clock Object contains the current date and time of the device	GET/PUT
Phone Book		
telecom/pb.vcf	Level 2 access (Access entire phonebook database)	GET/PUT
telecom/pb/luid/.vcf	Add new entry	PUT
telecom/pb/0.vcf	Own business card	GET/PUT
telecom/pb/info.log	Supported properties and memory info	GET
telecom/pb/luid/###.log	Change log	GET
telecom/pb/luid/cc.log	Change counter	GET
Calendar		
telecom/cal.vcs	Level 2 access	GET/PUT
telecom/cal/luid.vcs	Add new entry	PUT
telecom/cal/info.log	Supported properties and memory info	GET

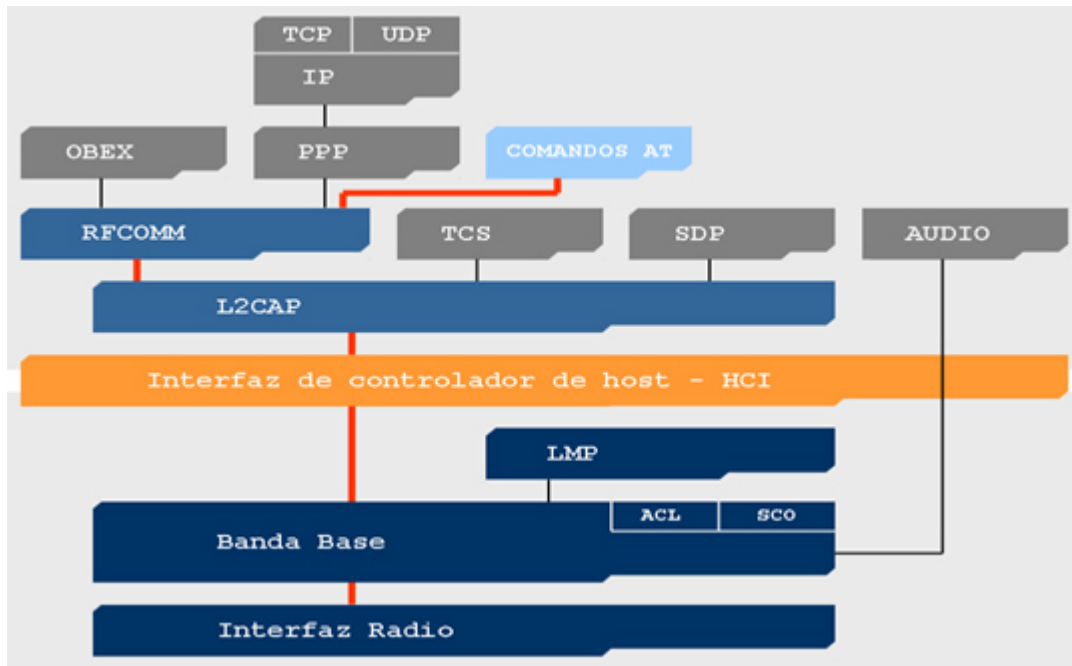
Fuente: Sony-Ericsson AT Commands Online Referente (Developer Guidelines, Octubre 2004)

5.2.1.4 Ataque BlueBug

Este tipo de ataque consiste en el establecimiento de una conexión RFCOMM a un canal oculto (no accesible por SDP) sin necesidad de autenticación y la ejecución de comandos AT en el terminal.

El esquema de la pila de protocolos Bluetooth, determina que desde el nivel RFCOMM se puede acceder a la capa de comandos AT, por lo que estableciendo una conexión RFCOMM a un determinado canal, el atacante puede iniciar una sesión de comandos AT con el teléfono móvil.

En la siguiente imagen se muestra el esquema bluetooth y donde se centra el ataque.



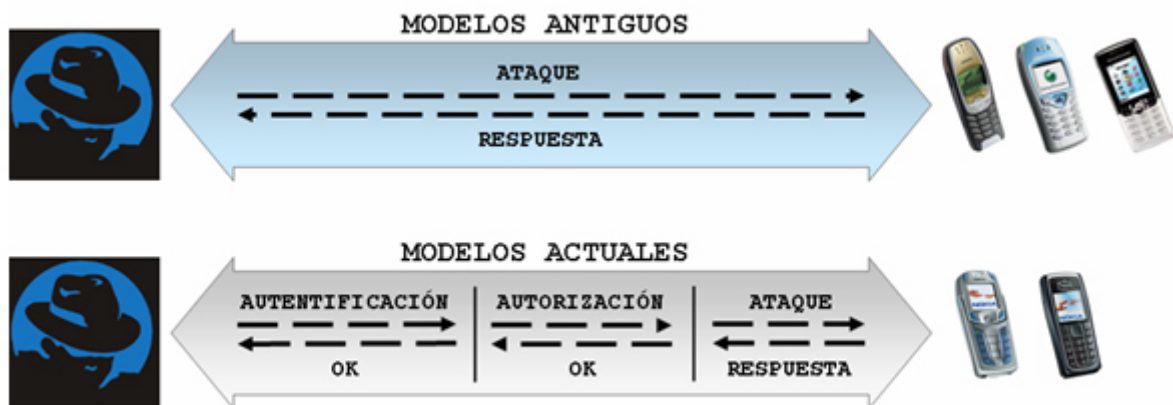
La posibilidad de ejecutar comandos AT con el terminal comprometido, puede permitir al atacante llevar a cabo varias acciones, tales como:

- Obtener información básica: Marca, modelo, IMEI,...
- Realizar llamadas de voz, desvío de llamadas,...
- Gestionar la agenda de contactos: Leer, escribir, borrar,...
- Acceder a la agenda de llamadas: Últimas llamadas perdidas, recibidas o realizadas.
- Gestionar los mensajes SMS: Leer, escribir y enviar, borrar,...

Este ataque es, sin duda, una de las vulnerabilidades más peligrosas y con mayor impacto en usuarios de teléfonos móviles Bluetooth, no sólo a nivel de privacidad, puesto que el infractor accede a toda la información privada del terminal, sino también a nivel económico, puesto que éste puede realizar todo tipo de llamadas telefónicas.

Como posible solución a este ataque, se podría restringir el acceso a los comandos AT desde el interfaz Bluetooth. Sin embargo, los propios fabricantes desarrollan aplicaciones para sincronizar un equipo PC con la agenda de contactos y la bandeja de entrada de mensajes SMS de los teléfonos móviles. La solución adoptada que adoptan para proteger los terminales, consiste en añadir mecanismos de autenticación antes de acceder a la conexión RFCOMM. De esta forma, es necesaria la intervención del propietario del teléfono móvil, resultando imposible llevar a cabo un ataque de forma transparente.

En la siguiente imagen se muestra el esquema/pasos del ataque en terminales antiguos y modernos.



5.2.1.5 Ataque Bluejacking

Este tipo de ataque consiste en el envío de mensajes no solicitados entre dispositivos Bluetooth.

Por lo general, resulta inofensivo, pero las personas que lo han sufrido han visto alterado el funcionamiento de su terminal, con las consiguientes molestias que esto provoca. Normalmente un bluejacker envía un mensaje de texto, aunque en los modelos de teléfonos más recientes es posible enviar también imágenes y sonido.

Con el aumento del uso de la tecnología Bluetooth en dispositivos móviles se ha fomentado la aparición de bluejackers y con ellos, software malicioso, cuyo objetivo es dificultar el funcionamiento del dispositivo mediante el envío de un virus troyano.

5.2.1.6 Explotación de vulnerabilidades específicas de terminales: HeloMoto y Blueline

Este tipo de ataque consiste en la incorrecta implementación de la lista de dispositivos de confianza de un terminal y sólo se da en los siguientes modelos de teléfono móvil: Motorola V80, v500 y v600.

El atacante inicia una conexión al Perfil de Carga de Objetos (OBEX Push Object) con la intención de enviar una tarjeta de visita *ovCard*. De forma automática y sin necesidad de interacción por parte del propietario del teléfono móvil, el dispositivo atacante es añadido a la lista de confianza del terminal. A partir de aquí, el infractor puede acceder a perfiles que requieran autorización, pero no autenticación, como es el caso del Perfil de Pasarela de Voz (Voice GatewayProfile). Una vez establecida la conexión con dicho Perfil, el atacante puede acceder a la ejecución de comandos AT en el teléfono móvil comprometido.

En algunos casos, el sistema provocaba una falsificación o spoofing del interfaz y sustituía el mensaje original de la ventana de notificación de conexión entrante, por cualquier otro texto deseado por el infractor. Esto se realizaba con sólo modificar el

nombre del dispositivo atacante por una cadena de caracteres maliciosa que contenía el carácter 0x0d para el salto de línea.

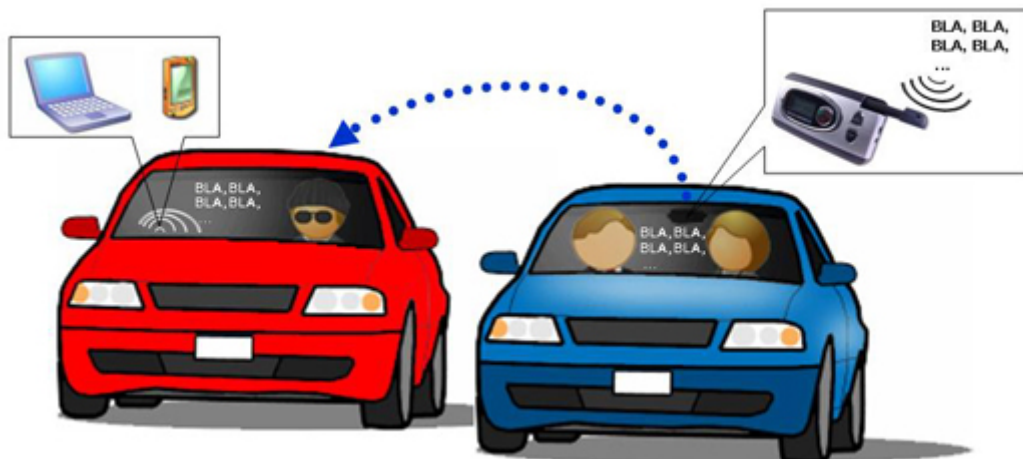
5.2.2 Ataques a implementación de Bluetooth en manos libres

5.2.2.1 Car Whisperer

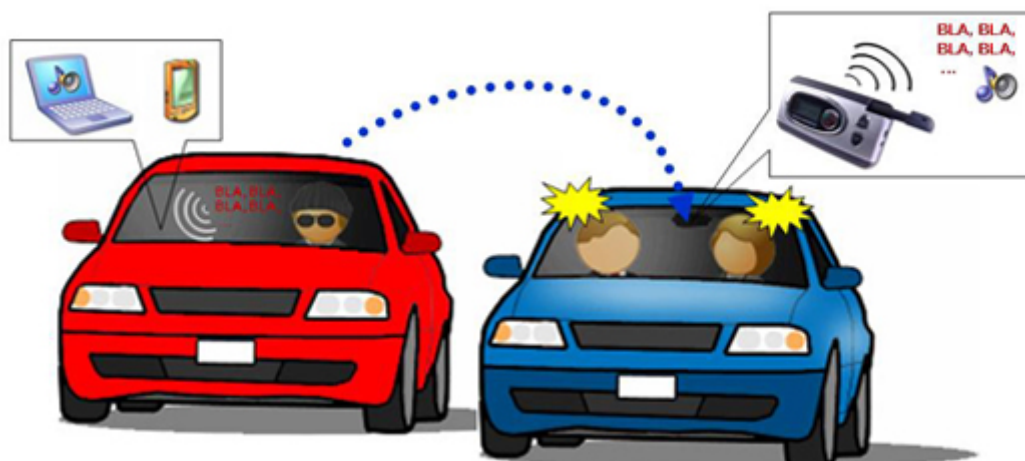
Este tipo de ataque consiste en usurpar la clave PIN de emparejamiento de los dispositivos Bluetooth con la finalidad de acceder a diversas funcionalidades del terminal. Se basa en los dispositivos Manos Libres de automóvil.

El hecho de incorporar una clave PIN por defecto en un dispositivo Bluetooth conlleva que cualquier usuario que averigüe dicha clave estándar puede emparejarse con el dispositivo y comunicarse con él de forma autorizada. En el caso de un Manos Libres, un atacante podría acceder a las funciones de audio implementadas en el terminal y llevar a cabo las siguientes acciones con fines maliciosos:

- Capturar el audio recogido por el micrófono del dispositivo, permitiendo escuchar conversaciones privadas en el interior del vehículo.



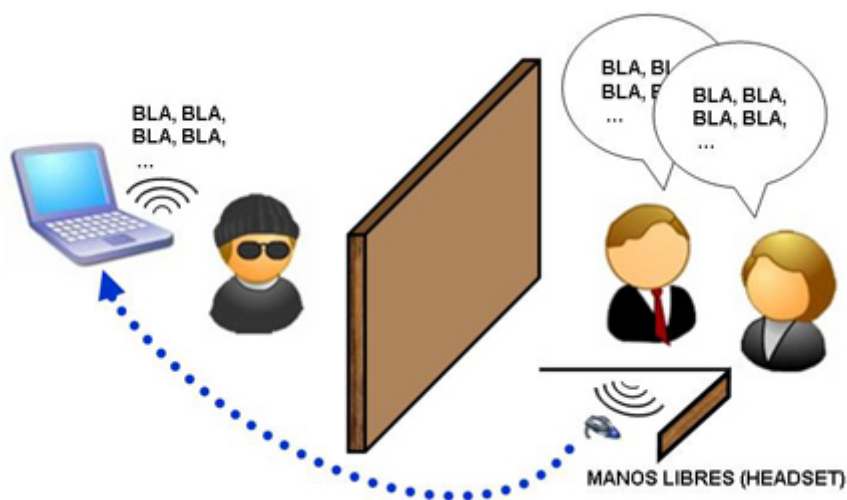
- Inyectar audio que sería reproducido por los altavoces del dispositivo, permitiendo proyectar mensajes de voz a los ocupantes del vehículo.



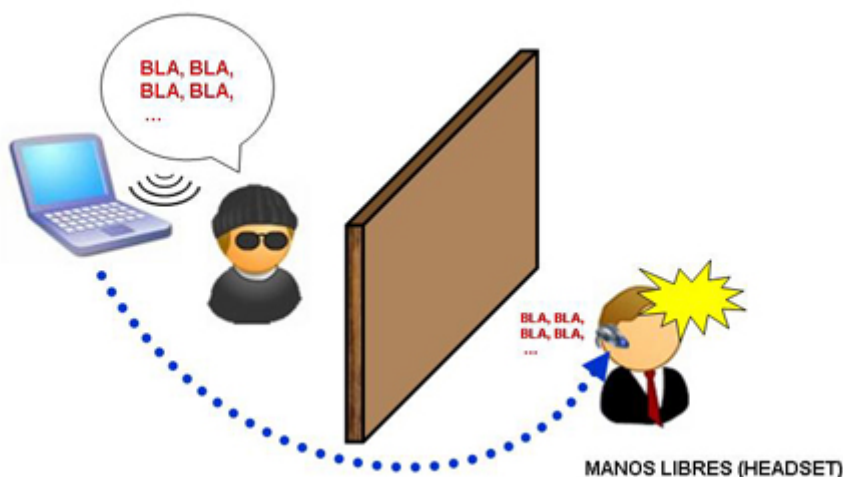
5.2.2.2 Ataque Headsets Hijacking

Este tipo de ataque consiste en usurpar el código de seguridad Bluetooth que los dispositivos Manos Libres Auriculares incorporan por defecto para acceder a sus funciones de audio y llevar a cabo las siguientes acciones con fines maliciosos:

- Capturar el audio recogido por el micrófono del dispositivo, permitiendo escuchar conversaciones privadas.



- Inyectar audio que sería reproducido por el auricular permitiendo proyectar mensajes de voz a los usuarios.



En algunos casos, incluso es posible cortar una conversación telefónica en curso e inyectar audio, para sorpresa del usuario.

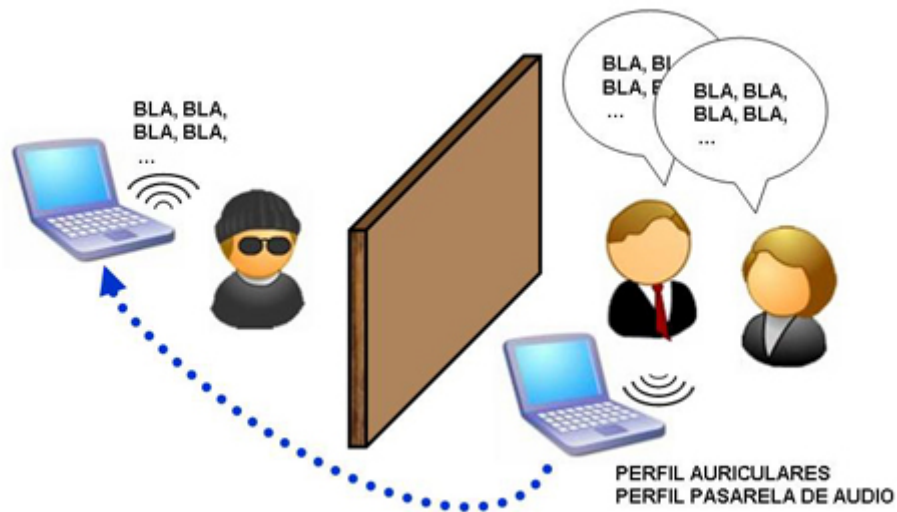
5.2.2.3 Ataque Laptop Audio Hijacking

Este tipo de ataque consiste en realizar una conexión remota a un PC con Bluetooth y utilizar el Perfil de Auriculares sin necesidad de autenticación.

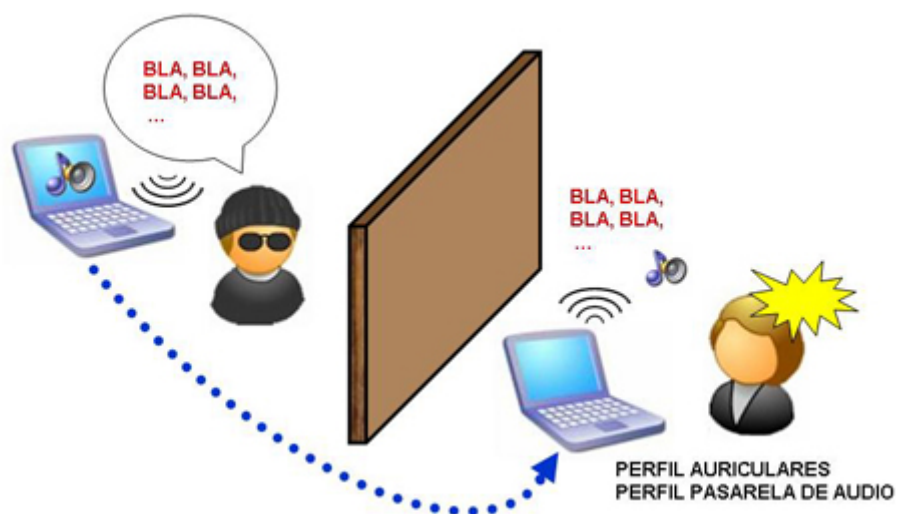
El modelo de uso para el Perfil de Auriculares denominado Pasarela de audio permite a un usuario configurar dos equipos Bluetooth y establecer una pasarela de audio entre los dos, de forma que el audio que reproduce el software de un dispositivo, se transmite al otro mediante el enlace SCO y puede ser proyectado por los altavoces del segundo. Así mismo, el audio recogido por el micrófono de un terminal se transmite al otro pudiendo ser grabado en un archivo de sonido.

Dicho ataque, permitiría a un atacante llevar a cabo las siguientes acciones con fines maliciosos:

- Capturar el audio recogido por el micrófono del dispositivo, permitiendo la escucha de conversaciones privadas.



- Inyectar audio y mensajes de voz que serían reproducidos por los altavoces del PC, para sorpresa del usuario del mismo.



Las víctimas potenciales de un ataque Laptop Audio Hijacking son todos aquellos usuarios de PC con Microsoft Windows que disponen de un dispositivo Bluetooth soportado por la pila de protocolos Widcomm.

En referencia a los usuarios con ordenador portátil o laptop, el caso es especialmente grave puesto que si un atacante consiguiera comprometer el Perfil de Auriculares, tendría acceso al control del micrófono y podría grabar conversaciones privadas. En el caso que el equipo comprometido no incluyera micrófono, el atacante sólo podría inyectar audio que sería proyectado por los altavoces del PC.

5.3 Ataques a la tecnología RFID

5.3.1 Ataque a los elementos tecnológicos del RFID

Los riesgos para la seguridad de la tecnología RFID son aquellos derivados de acciones encaminadas a deteriorar, interrumpir o aprovecharse del servicio de forma maliciosa. Con este tipo de actos se perseguirá un beneficio económico o bien un deterioro del servicio prestado.

La forma más simple de ataque a un sistema RFID es evitar la comunicación entre el lector y la etiqueta, pero también existen otras formas de ataque más sofisticadas, cuyo blanco son las comunicaciones en radiofrecuencia.

5.3.1.1 Aislamiento, Desactivación o destrucción de etiquetas

Este tipo de ataque consiste en impedir la correcta comunicación lector-etiqueta. Esto se consigue mediante la introducción de la etiqueta en una “jaula de Faraday” o creando un campo electromagnético que interfiera en el lector.

Del mismo modo, también se pueden inutilizar las etiquetas sometiéndolas a un fuerte campo electromagnético que destruye la sección más débil de la antena e invalida el mecanismo. Si se dispone de los medios técnicos necesarios, se pueden inutilizar las etiquetas de protección antirrobo de los productos, favoreciéndose así su sustracción.

5.3.1.2 Suplantación de etiquetas

Este tipo de ataque consiste en el envío de datos falsos que suplantán a los correctos.

Este tipo de ataque puede servir para sustituir etiquetas permitiendo la obtención de artículos caros con etiquetas reemplazadas de productos más baratos. Además, aplicado a la cadena de distribución, puede llegar a acarrear un fraude de grandes dimensiones si se sustituyen grandes cantidades de mercancías.

5.3.1.3 Inserción

Este tipo de ataque consiste en la inserción de comandos ejecutables en la memoria de datos de una etiqueta pudiendo inhabilitar lectores y otros elementos del sistema.

La finalidad de este tipo de ataque será la desactivación del sistema o la invalidación de parte de sus componentes, permitiendo algún tipo de fraude, o una denegación de servicio sin más.

5.3.1.4 Repetición

Este tipo de ataque consiste en enviar al lector RFID una señal que reproduce la referente a una etiqueta lícita y que ha sido capturada mediante escucha.

Este ataque permitirá suplantar la identidad que representa una etiqueta RFID.

5.3.1.5 Clonación de la tarjeta RFID

Este tipo de ataque consiste en copiar los datos transmitidos entre una etiqueta y un lector. Dichos datos se replican en otra etiqueta RFID para ser utilizados posteriormente.

5.4 Ataques a la tecnología NFC

La tecnología NFC tiene como principal punto de ataque, su medio de comunicación, el aire. De todos modos, cabe destacar que se trata de un sistema cuyas aplicaciones, se encuentran, en su mayoría en periodo de pruebas, por lo que no será hasta que su uso se torne masivo cuándo empiecen a surgir problemas...

5.4.1 Redirección a sitios maliciosos a través de las etiquetas NFC

Este tipo de ataque consiste en el redireccionamiento de los usuarios, mediante la utilización de códigos QR hacia sitios web que contienen exploits con finalidades fraudulentas, tipo phishing, envío de virus,... Es por ello que hay que tener precaución a la hora de abrir estos enlaces.

De hecho, este es el motivo por el que se incluye el RTD firma, en los datos de las etiquetas. Puesto que de ese modo, un fabricante puede firmar el contenido de un campo URI, permitiendo al usuario conocer la autenticidad del sitio web donde lo conduce la etiqueta NFC.

Una buena práctica para solventar esta ataque, sería no acceder a URIs sin firmas contenidas en etiquetas NFC.

6. Mitigación de los riesgos y ataques a las comunicaciones inalámbricas.

En base a la naturaleza de los protocolos de comunicaciones inalámbricas y los requerimientos de seguridad, vamos a proceder a evaluar los pros y contras de las distintas medidas de seguridad de cada uno de ellos, así como indicar, des de nuestro punto de vista, las medidas más eficientes para mitigar los riesgos. Adicionalmente se indicarán aquellos aspectos de mejora que se podrían aplicar en el estándar para mejorar la postura de seguridad de estos.

6.1 Mitigación de los riesgos y ataques en el estándar 802.11.

Sin lugar a dudas, esta es la tecnología que permite más opciones de configuración del nivel de seguridad de la red, más allá de la protección del propio dispositivo.

A continuación vamos a analizar los pros y contras de las líneas de actuación para proteger dicha tecnología:

Control	PROS	CONTRAS
WEP (Wired Equivalent Privacy)	Compatibilidad con casi todos los dispositivos.	Fácil vulnerabilidad, incluso por personas con pocos conocimientos técnicos.
WPA (Wi-fi Protected Acces).	Gran simplicidad de aplicación en relación a los buenos resultados de protección que ofrece.	Fácil vulnerabilidad mediante ataques de fuerza bruta, en caso de utilizar Pre-Share Key débiles.
WPA2 (Wi-Fi Protected Access).	Sistema que ofrece el mayor grado de seguridad del protocolo.	Existencia de incompatibilidades con ciertos dispositivos que suponen una incorrecta implantación. De igual modo, fácil vulnerabilidad mediante ataques de fuerza bruta, en caso de utilizar Pre-Share Key.
Filtros por MAC	Limitación de acceso a los dispositivos permitidos.	Fácil vulnerabilidad dada la sencillez del sistema y el gran trabajo de gestión que conlleva.
Autenticación mediante Servidores AAA (Authentication Authorization Accounting)	Autenticación robusta. Sistema que ofrece el mayor grado de seguridad para entornos corporativos grandes y medios.	Difícil aplicación en pequeñas empresas y usuarios particulares, dado el gran trabajo de gestión que conlleva.
Implantación de sistemas de detección y protección de Intrusiones o Wireless Intrusion/detection system.	Visibilidad del comportamiento de los dispositivos en la red.	Difícil gestión autónoma del sistema, con la consecuente necesidad de capital humano para llevarlo a cabo.
Segregación de la red WI-FI mediante Firewall y VPN.	Máximo desglose de la red interna Wi-Fi.	Difícil aplicación en entornos corporativos, dado el gran trabajo de gestión que conlleva.

6.1.1 Valoración personal a cerca de los mejores métodos para mitigar los riesgos del protocolo 802.11.

Una vez analizados los pros y contras de las medidas de seguridad a aplicar en redes Wi-Fi, considero que las más favorables a emplear en entornos privados son aquellas que limitan el acceso a la red mediante contraseñas y la ocultación del nombre de la misma, dado que creo que es una forma sencilla de reducir los ataques con patrones de creación de contraseñas y limitar las intrusiones a atacantes con pocos conocimientos técnicos.

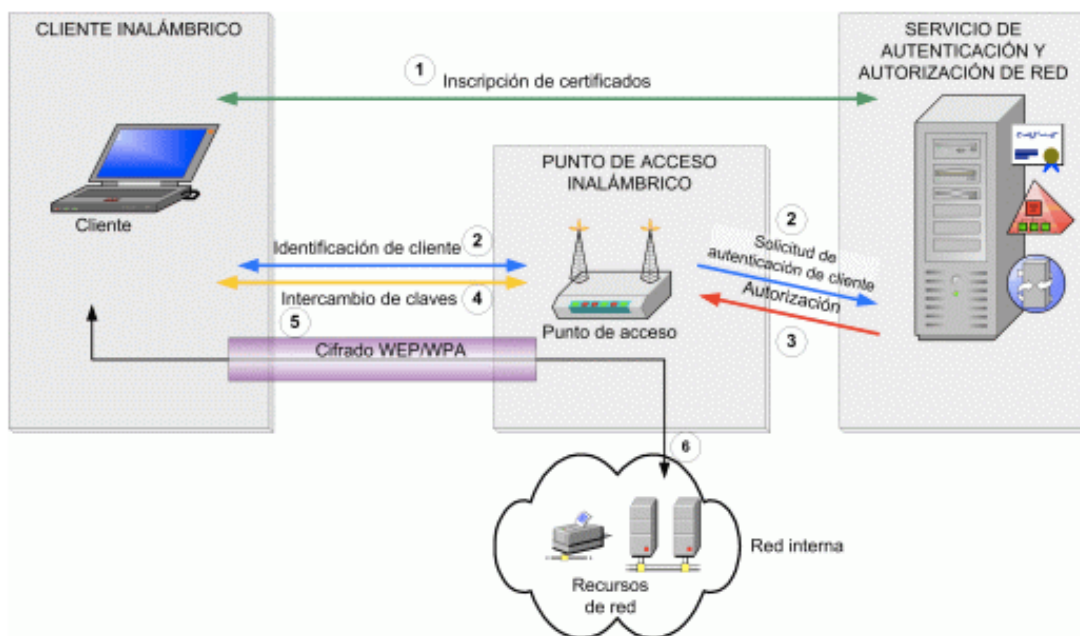
Del mismo modo, también considero de gran utilidad el empleo de un protocolo de seguridad robusto. Creo que el mínimo en estos casos, debería ser WPA-PSK, aunque en la medida de lo posible se debería emplear WPA2, dados los resultados ofrecidos en materia de seguridad.

Si su aplicación se refiere a nivel empresarial la mejor medida a adoptar, en mi opinión, sería la creación de una infraestructura Wifi que incluyera los elementos específicos para un buen control de la red.

Dicha infraestructura estaría compuesta por:

- **Puntos de acceso 802.11x** que permitiesen realizar funciones de control de acceso y cifrado de datos entre clientes wireless y puntos de acceso (AP) para la realización segura del intercambio de claves.
- **Servicio de Autenticación RADIUS**, que recibiese las solicitudes de autenticación de los clientes y realizase las consultas de credenciales y certificados del usuario en el servicio de directorio LDAP.
- **Directorio LDAP**, que almacenase de forma centralizada las cuentas de usuarios, junto con las políticas de control de acceso.
- **Autoridad de Certificación**, que permitiera emitir los certificados digitales de los usuarios, cuya parte pública estaría almacenada en el directorio LDAP y la parte privada en el equipo del usuario.

En la siguiente imagen se puede observar un esquema de la solución propuesta:



6.1.2 Posibles aspectos a mejorar del estándar 802.11.

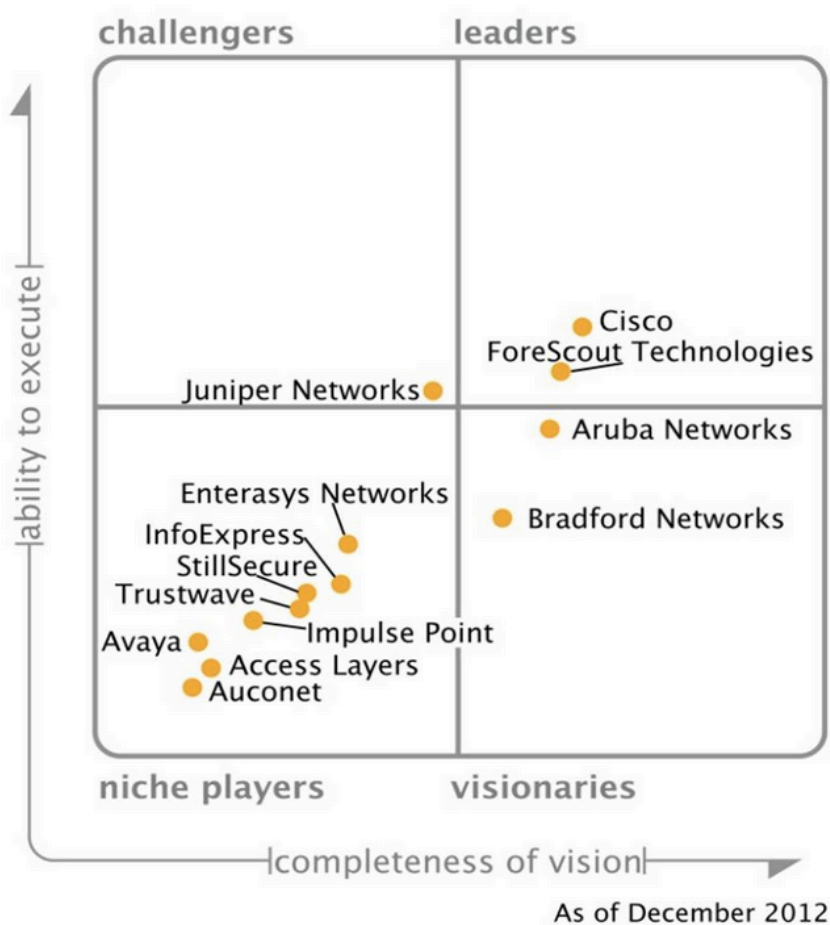
En referencia a las medidas de protección propuestas para la tecnología Wi-Fi, creo que cabe destacar el gran número de opciones disponibles y la complejidad en la aplicación de muchas de ellas.

En mi opinión es el protocolo con mayor dificultad a la hora de aportar mejoras, puesto que tiene un gran número de medidas de seguridad a aplicar para crear un entorno protegido.

De todos modos, me gustaría indicar una medida que aunque no es propia de WI-FI, creo que permite obtener un nivel de control de acceso extra, muy eficiente en entornos corporativos críticos. Se trata de la implantación de sistemas de Network Access Control más conocidos como NAC.

Dichos métodos, permiten aplicar controles de integridad (software antivirus actualizados, políticas de contraseña, aplicaciones específicas...) que permiten obtener una visibilidad y control riguroso sobre quién, cómo y cuando se conecta a la red. Pero, en ocasiones, suponen un foco de problemas para los equipos de atención a los usuarios, por lo que, en mi opinión, siempre se deberá buscar un equilibrio entre seguridad y usabilidad.

En el siguiente gráfico se puede observar una comparativa de sistemas NAC realizada por gartner.



6.2 Mitigación de los riesgos y ataques en el protocolo Bluetooth.

Actualmente existen varias versiones del protocolo Bluetooth, pero tal como hemos visto anteriormente, su principal utilización se lleva a cabo por usuarios de dispositivos móviles. Es por ello que las medidas de seguridad que se aplican, están muy orientadas al empleo de las mismas y no tanto a las especificaciones del protocolo.

Cabe destacar que las medidas que a continuación se indicarán son medidas simples y de aplicación inmediata que deberían formar parte de la conducta habitual del uso de dicha tecnología:

Control	PROS	CONTRAS
Activación Bluetooth en el dispositivo sólo cuando sea necesario.	Control del uso por parte del usuario.	Perdida de tiempo para el usuario.
Configuración del dispositivo en modo oculto o non discoverable.	Presencia inadvertida para usuarios básicos.	Fácil vulnerabilidad para usuarios maliciosos avanzados.
Configuración del dispositivo para que utilice la función de cifrado en todas las comunicaciones.	Confidencialidad garantizada en el intercambio de mensajes.	N/A
Utilización de un nombre de dispositivo que no sea representativo de la marca y del modelo del mismo.	Entorpecimiento en el reconocimiento a usuarios básicos.	Fácil vulnerabilidad para usuarios maliciosos avanzados.
Rechazo de conexiones entrantes de dispositivos desconocidos.	Control de las conexiones por parte del usuario.	Utilización problemática para el usuario.
Configuración de todos los perfiles soportados por el dispositivo para que requieran autenticación ante cualquier intento de acceso.	Control sobre todas las funciones del protocolo.	Utilización problemática para el usuario.
Verificación periódica de la lista de dispositivos de confianza y eliminar aquellas entradas con los que habitualmente no se establece conexión.	Control de las conexiones por parte del usuario.	Utilización problemática para el usuario.
Utilización en la medida de lo posible de claves PIN de longitud extensa, hasta 16 bytes.	Autenticación robusta.	Utilización problemática para el usuario.

6.2.1 Valoración personal a cerca de los mejores métodos para mitigar los riesgos del protocolo Bluetooth

Una vez realizados los pros y contras de cada una de las medidas referentes a la tecnología Bluetooth, considero que la más apropiada tanto en entornos privados, como empresariales, es la utilización de un PIN de más de 16 dígitos para reducir los posibles ataques por fuerza bruta.

De igual modo, en entornos particulares, creo que puede resultar de gran utilidad la activación del dispositivo cada vez que sea necesario, evitando de ese modo el riesgo de captura de la negociación.

En los entornos empresariales, destacaría también, la configuración de los perfiles de manera que todas las funciones soliciten autenticación, y de ese modo limitar el abuso de los terminales por parte de usuarios maliciosos.

6.2.2 Posibles aspectos a mejorar en el estándar Bluetooth.

En referencia a las medidas de protección propuestas para la tecnología Bluetooth, creo que se caracterizan por una gran simplicidad, en muchos casos excesiva, hecho que conlleva que cualquier atacante puede realizar usurpaciones de información con relativa facilidad.

De igual forma considero que es demasiado elevada, la responsabilidad que recae sobre el usuario en materia de seguridad, puesto que debe ser él quién se encargue de la activación/desactivación del sistema en todo momento.

Por ello, creo que una mejora en el estándar sería la obligatoriedad en la utilización de PIN's aleatorios y la implantación del algoritmo AES, que proporcionaría mecanismos más robustos que los utilizados actualmente.

Por otro lado, los dispositivos deberían tener activadas por defecto las tres funciones del estándar: autenticación, autorización y cifrado, no dejando la responsabilidad de la activación al usuario final.

6.3 Mitigación de los riesgos y ataques en el protocolo RFID.

El principal ataque que puede sufrir la tecnología RFID, es el intento de lectura de los datos personales almacenados en alguno de sus dispositivos.

Para evitar dicho acceso indeseado, existen varias medidas, las cuales se identifican en la siguiente tabla:

Control	PROS	CONTRAS
Utilización de etiquetas watchdog.	Detección de intentos de lectura y escritura indeseados, con la consiguiente posibilidad de realizar un bloqueo.	Utilización problemática para los usuarios. Imposibilidad de aplicación en entornos móviles de lectura y escritura.
Utilización de Firewalls RFID.	Obtención de buenos resultados en entornos de máxima seguridad.	Imposibilidad de aplicación en entornos móviles de lectura y escritura.
Utilización de etiquetas de un solo uso.	Garantía de confidencialidad dado el uso único.	Imposibilidad de aplicación en entornos móviles de lectura y escritura. Coste de implantación elevado.
Aplicación de medidas de autenticación en etiquetas y lectores.	Eliminación de las lecturas no adecuadas.	Complejidad de aplicación en entornos móviles de lectura y escritura.
Aplicación de métodos de cifrado de comunicaciones, diseñados por proveedores. (por ejemplo aplicación de la seguridad Mifare de Phillips).	Limitación en la captura de información.	Existencia de algoritmos de fabricantes con vulnerabilidades reconocidas.

6.3.1 Valoración personal a cerca de los mejores métodos para mitigar los riesgos del protocolo RFID.

Una vez realizados los pros y contras de cada una de las medidas de seguridad de la tecnología RFID, considero que el mejor procedimiento a aplicar en entornos privados, es la utilización de fundas que impidan la lectura de las tag RFID personales.

De igual modo, en entornos empresariales creo que las medidas más adecuadas son la activación de etiquetas watchdog que permitan disponer de un registro de la actividad y poder así, actuar en consecuencia. Y el empleo de mecanismos de cifrado y autenticación para definir y analizar el uso de las etiquetas.

6.3.2 Posibles aspectos a mejorar del estándar RFID.

En referencia a las medidas de protección propuestas para la tecnología RFID, creo que existe una gran complejidad a la hora de aplicar un cifrado robusto, dada la limitación en el tiempo de ejecución y la energía necesaria para llevarlo a cabo. Por todo ello, creo que en las etiquetas pasivas, la aplicación de cifrado, no es factible y deberían limitarse los campos modificables o las utilidades aplicables, en función de la utilidad aplicada.

De igual forma, creo que sería conveniente estudiar para el estándar EPCglobal y ISO/IEC 18000, un sistema de cifrado y autenticación que permitiera fortalecer las comunicaciones en entornos más críticos. Por ejemplo, se podría adoptar un mecanismo de cifrado de 32 bits, a modo de reto, mediante la aplicación de un esquema de claves privadas y públicas, configuradas en la instalación de los sistemas. El estándar sería similar a lo aplicado por Mifare pero con la diferencia que los retos no viajarían en claro, complicando de ese modo el criptoanálisis.

De todos modos, debemos tener en cuenta que dada la longitud de bits que podemos utilizar en esta tecnología, ésta siempre será susceptible de rotura por fuerza bruta.

6.4 Mitigación de los riesgos y ataques en el protocolo NFC.

La tecnología NFC se encuentra en proceso de desarrollo, por lo que es difícil establecer unas metodologías de seguridad precisas y concretas. Pero sí se pueden definir una serie de líneas de actuación para proteger en gran medida dicho protocolo, las cuales se detallan en la siguiente tabla:

Control	PROS	CONTRAS
Activación del NFC en aquellos momentos en los que el usuario vaya a utilizar dicha tecnología.	Control de su uso por parte del usuario.	Perdida de tiempo para el usuario.
Actualización periódica del sistema operativo y sus aplicaciones.	Elevado nivel de protección para los sistemas, puesto que supone disponer de las últimas novedades en materia de seguridad.	Complejidad de disponer constantemente de la última versión.
Instalación de aplicaciones limitada a aquellas que sean de total confianza.	Control sobre el funcionamiento real de la aplicación.	Limitación en el uso de aplicaciones por parte del usuario.
Lectura limitada a etiquetas NFC.	Control sobre la confianza del contenido de las etiquetas.	Limitación en el uso del terminal NFC.
Utilización de cifrado en el almacenamiento de información y en comunicaciones.	Protección de la información confidencial del usuario.	Posibilidad de pérdida de datos en caso de avería del terminal.
Inutilización del modo pasivo del terminal.	Limitación en la lectura de datos.	Limitación del uso del terminal NFC.

Control	PROS	CONTRAS
Limitación de las cantidades de pago con móvil.	Limitación del impacto del fraude en caso de robo del terminal o de los datos de pago.	Limitación del uso del terminal NFC.

6.4.1 Valoración personal de los métodos de mitigación NFC.

Una vez realizados los pros y contras de cada una de las medidas para garantizar la seguridad de la tecnología NFC, creo que la mejor metodología a aplicar tanto en este protocolo como en los otros tres, es la actualización del sistema operativo y la utilización de aplicaciones obtenidas de sitios oficiales. En mi opinión, son las medidas más sencillas y básicas para el usuario y también, las que ofrecen mejores resultados, puesto que al igual que los ataques sufren continuos cambios, en paralelo, también lo hacen las medidas de protección aplicadas a los sistemas.

En cuanto a la activación y desactivación del aplicativo, por parte del usuario, creo que al igual que en el Bluetooth, no es una medida práctica, puesto que supone al cliente una gran pérdida de tiempo, que en muchas ocasiones supondrá no llevarlo a cabo.

De igual modo, en el caso del pago por móvil las entidades participantes deben tener presente los riesgos a los que está expuesto el sistema y actuar en consecuencia, creando aplicaciones seguras que cifren los datos, enmascarando información en las pantallas de los terminales, y aplicando límites en las cuantías de pago. Todo ello para proteger al máximo los intereses del usuario.

6.4.2 Posibles aspectos a mejorar del estándar NFC.

En referencia a las medidas de protección propuestas para la tecnología NFC, creo que actualmente todos los componentes de la arquitectura de pago están intentando ganar su sitio. Por lo que creo que sería necesario definir un estándar para determinar una arquitectura base, en la cual se obligue a aplicar el cifrado a toda la información confidencial del usuario, protegiendo su acceso mediante autenticación y autorización.

7. Conclusión

A lo largo del presente proyecto he desarrollado el estudio de los protocolos 802.11 (WIFI), Bluetooth, RFID y NFC, en base a los elementos de seguridad de cada uno de ellos. He estructurado dicho estudio, en el análisis de las principales características técnicas de cada uno de ellos, seguidas de los principales ataques que actualmente se están produciendo y las respuestas que se han llevado a cabo hasta el momento.

Una vez, establecida una visión global de la seguridad de dichos estándares hasta la actualidad, he querido realizar un análisis crítico de todo ello. De ese modo, ha valorado pros y contras, y he desarrollado posibles aspectos de mejora que podrían suponer un mayor nivel de seguridad en las comunicaciones sin hilos.

Por todo ello, creo que he constatado que la seguridad es una prioridad en todos los protocolos, por lo que las tecnologías implementan mejores y más robustas soluciones de seguridad, siendo en este caso la tecnología 802.11 (WIFI) la que más medidas presenta, y siendo el RFID, por limitaciones de la tecnología, la que menos opciones ofrecen al usuario.

En mi opinión, la tecnología que presenta las medidas de seguridad más robustas es la 802.11 (WIFI), la cual ha tenido que evolucionar y adaptarse de una forma más rápida a los números vectores de ataques que ha ido sufriendo. Adicionalmente el protocolo NFC es un recién llegado, pero pronto será un foco de análisis y ataque por parte de investigadores y usuarios maliciosos, debido a la funcionalidad de pago por el móvil, un caramelo para los defraudadores.

Por otro lado, las medidas a aplicar en cada situación depende del uso que se le quiera dar a dichos protocolos. En el caso del uso personal, se puede concluir que los entornos inalámbricos en general son seguros y que basta con seguir una serie de recomendaciones básicas tales como, la actualización de los sistemas, el uso de contraseñas robustas y la modificadas periódicamente de estas, para reducir riesgos. En el caso del protocolo NFC, es necesario que el usuario considere el terminal móvil como un medio de pago más, y actué en consecuencia si quiere realizar pagos por NFC.

Por último, la tendencia en el entorno empresarial, es la de implementar sistemas de gestión centralizada (la autenticación por radius y PKI, el uso de WPA2, la actualización de los sistemas, el uso de sistemas WIDS y y la centralización mediante MDM) de los dispositivos móviles y redes WIFI, que permita visibilidad sobre el acceso a la red y cubrir incidentes de pérdida, robo y recuperación y confidencialidad de la información accesible.

8. Bibliografía

Bibliografía, artículos y recursos web utilizados para la realización de este proyecto final de carrera:

- IEEE Standard
 - <http://www.ieee.org/index.html>
- Bluetooth
 - <http://www.bluetooth.com/Pages/Bluetooth-Home.aspx>
- Bluehack: the Spanish Bluetooth Security Group
- Seguridad mobile
 - <http://www.seguridadmobile.com/>
- Instituto Nacional de Tecnologías de la Comunicación
 - www.inteco.es
- Security in Near Field Communication (NFC) - Strengths and Weaknesses of Ernst Haselsteiner and Klemens Breitfuß
- NIST National Institute of Standards and Technology
 - www.nist.gov
 - NIST SP800-115 Technical Guide to Information Security testing and Assesment.
 - NIST 800-101 – Guidelines on Cell Phone Forensics.
- CCN-CERT
 - www.ccn-cert.cni.es
- NFC Forum
 - <http://www.nfc-forum.org/home/>
- Security At Work
 - <http://www.securityartwork.es/2010/02/03/hacking-rfid-rompiendo-la-seguridad-de-mifare-ii/>
- Material oficial de Microsoft
 - www.microsoft.com