Seguridad avanzada en redes wireless

Conceptos básicos

INTRODUCCIÓN

- Una **red inalámbrica** (*wireless network* en inglés) es aquella que permite comunicar dos o más terminales a través de un medio de transmisión no guiado, es decir, sin necesidad de cables. En su lugar, se envían ondas electromagnéticas por el vacío entre dos antenas.

- Tiene muchas ventajas de movilidad y económicas, pero tiene el problema de la seguridad.

- La falta de seguridad es un problema grave que no tiene la atención necesaria por parte de los administradores de redes.

- Es común encontrar redes en las cuales el acceso a Internet se protege adecuadamente con un firewall bien configurado, pero en el interior de la red existen puntos de acceso inalámbrico totalmente desprotegidos e irradiando señal hacia el exterior del edificio.

- Cualquier persona que desde el exterior capte la señal del punto de acceso, tendrá acceso a la red de la compañía, con la posibilidad de navegar gratis en Internet, emplear la red de la compañía como punto de ataque hacia otras redes para luego desconectarse y no ser detectado, robar software y/o información, introducir software maligno entre muchas otras cosas.

Conceptos básicos

INTRODUCCIÓN

- **IEEE 802** es un estudio de estándares elaborado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) que actúa sobre Redes de ordenadores

- El estándar 802.11 está dedicado a las redes wifi. Este trabajo busca presentar las tecnologías existentes para mejorar el nivel de seguridad en las redes inalámbricas 802.11 con sus ventajas, desventajas y escenarios de aplicación así como la descripción de nuevas tecnologías en desarrollo para este fin.

- El estándar 'IEEE 802.11' define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

- Inicialmente se utilizaron las redes WEP, que utilizan un mecanismo de encriptación especificado en el estándar IEEE 802.11, que garantiza la seguridad entre los usuarios y los puntos de acceso. Este mecanismo no resultó muy seguro, y se utiliza la encriptación WPA, que no es la solución, pero es mejor.

- Hoy día la seguridad ha dejado de ser una opción y se ha convertido en un requisito indispensable para el desarrollo de empresa, organización o incluso hogar.

Conceptos básicos

INTRODUCCIÓN

- En general, las redes inalámbricas son inseguras debido a que su medio de transporte es el aire.
- Este trabajo busca presentar las tecnologías existentes para mejorar el nivel de seguridad en las redes inalámbricas 802.11 con sus ventajas, desventajas y escenarios de aplicación así como la descripción de nuevas tecnologías en desarrollo para este fin.

Actualmente se vienen configurando una serie de aspectos para mantener la seguridad en una red del tipo wireless como por ejemplo los siguientes:

· ACL (Access Control List).
· SSID (Service Set Identifier).
· WEP (Wired Equivalent Protocol).
· WPA (Wi-Fi Protected Access).

❑ En un futuro próximo, un número cada vez mayor de sistemas estarán implementando redes basadas en conexiones inalámbricas, creando así oportunidades adicionales para rastreos y otros tipos de conductas nefastas.

❑ Debido a la conexión de las redes inalámbricas con las redes de cable, la seguridad tiene necesariamente que ser la piedra angular de cualquier implementación inalámbrica, especialmente cuando esté en juego la seguridad de la información gubernamental. Si la seguridad no es la primera prioridad, los sistemas inalámbricos terminarán siendo "El talón de Aquiles de las redes"

Conceptos básicos

DEFINICIONES

- ✓ **Wi-Fi (Wireless Fidelity).** Marca creada por la WECA (*Wireless Ethernet Compatibility Alliance),* hoy conocida como *Wi-Fi Alliance ,* para fomentar una tecnología inalámbrica compatible con multitud de equipos. Se trata de un sistema de envío de datos a través de ondas de radio basado en la norma IEEE 820.11

  Se basa en el modelo de capas OSI.

  7. Capa de aplicación
  6. Capa de presentación
  5. Capa de sesión
  4. Capa de transporte
  3. Capa de red
  2. Capa de enlace de datos
  1. Capa física.

- ✓ **Dirección IP.** La dirección IP es una etiqueta jerárquica a cada host dentro de protocolo TCP/IP. Esta debe ser diferente al resto de direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host.

Conceptos básicos

DEFINICIONES

Las direcciones IP se clasifican en:

- **Publicas:** Aquellas direcciones que son visibles en todo internet.
- **Privadas:** Visibles únicamente por otros equipos de la propia red o de otras redes privadas interconectadas por routers. En un ataque a una red inalámbrica trabajaremos con IP's de éste tipo. Un router dentro de una red privada asigna IP's privadas de mediante el protocolo DHCP.

✓ **Dirección física MAC (Medium Access Control)** Código exclusivo de 12 caracteres hexadecimales que los fabricantes graban en los dispositivos de red (adaptadores de red o puntos de acceso) para poder identificarlos de forma inequívoca en redes Ethernet y Wi-Fi, entre otras. Los 6 primeros bytes identifican al fabricante del dispositivo y los 6 restantes corresponden al número de serie.

MAC opera en la capa 2 del modelo OSI y, al ser el sistema operativo el que gestiona esta capa, es posible modificar la dirección MAC de los adaptadores de red.

Conceptos básicos

DEFINICIONES

- ✓ SSID. (Service Set Identifier). Código de 32 caracteres alfanuméricos que identifica paquetes de datos como parte de una WLAN. Si la red incorpora una estructura intermedia, AP, Router, … entonces utilizan una versión de este código llamado ESSID (Extended Service Set Identifier). Cada red wireless tiene un ESSID que la identifica. El ESSID consta de cómo máximo 32 caracteres y es case-sensitive (sensible a mayúsculas).

- ✓ BSSID. (Basic Service Set Identifier) Identificación de los clientes (ordenadores) conectados a un punto de acceso. Es la dirección MAC del Punto de Acceso, la emplean las tarjetas wireless para identificar y asociarse a redes inalámbricas.

- ✓ Beacon Frames. Son información de los AP, que mandan constantemente anunciando la red, para que los clientes móviles puedan detectar su presencia y conectarse a la red wireless. Si capturamos las tramas de una red wireless podremos ver que normalmente el AP manda el ESSID de la red en los BEACON FRAMES

Conceptos básicos

DEFINICIONES

Protocolo ARP (Adress Resolution Protocol).

La misión del protocolo ARP es obtener la dirección física (MAC)de un ordenador a partir de su dirección IP.

El protocolo ARP funciona de la siguiente forma: Imaginemos que queremos enviar datos a un equipo del que conocemos su IP. En ese caso enviamos un mensaje ARP preguntando a todas las máquinas de nuestra red si conocen la dirección física de la máquina con dirección IP con la que queremos comunicarnos. Y si algún dispositivo conoce la dirección que estamos buscando, o el propio equipo ha recibido la trama ARP de difusión, éste responde directamente al ordenador interesado con la dirección física que buscaba.

Las preguntas ARP son de difusión y estas preguntas llevan además la dirección IP y la dirección física de la máquina que pregunta, mientras que las respuestas se envían directamente a la máquina que formuló la pregunta.

Conceptos básicos

DEFINICIONES

Estandares Wifi

WiFi (Wireless Fidelity) es el nombre con el que se bautizó el estándar que describe los productos WLAN basados en los estandares IEEE 802.11.

Dicho modelo fue desarrollado por un grupo de comercio, que adoptó el nombre de "WiFi Alliance"

El estándar 802.11 vio la luz en Junio de 1997 y se caracteriza por ofrecer velocidades de 1 y 2 Mbps, un sistema de cifrado sencillo llamado WEP (Wired Equivalent Privacy) y operar en la banda de frecuencia de 2.4 Ghz; en dos años, septiembre de 1999, aparecen las variantes 802.11a y 802.11b que ofrecen velocidades de 54 y 11 Mbsp respectivamente. Pronto se pondrían de manifiesto las carencias a nivel de seguridad de estos estándares.

La familia 802.11 se encuentra compuesta, a día de hoy, por los siguientes estándares(protocolos):

- ✓ 802.11 legacy. Es la versión original del estándar IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2 megabits por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR).
- ✓ 802.11a. Aprobada en 1999. es una ampliación de la anterior. Opera en la banda de 5 Ghz. Utiliza modulación OFDM: Multiplexación por división de frecuencias ortogonal, llegando a velocidades de 20Mbits/sg.
- ✓ 802.11b. Opera en la banda de 2,4 GHz, con velocidades de 11 Mbps.

Conceptos básicos

DEFINICIONES

Estandares Wifi

- ✓ 802.11c. Menos usado por el público general. Define las características de AP.
- ✓ 802.11d. Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias). Permite el uso internacional de redes locales.
- ✓ 802.11e. Define conceptos de Calidad de servicio (QoS).
- ✓ 802.11f. Define el protocolo de conexión entre puntos de acceso (AP) para que sean más compatibles. Utiliza el protocolo IAPP: Inter Access Point Protocol, que permiten a un usuario en movimiento cambiarse de AP.
- ✓ 802.11g. Utliza la banda de 2,4 GHz, 36 o 54 Mbps. OFDM: Multiplexación por división de frecuencias ortogonal. Es compatible con el estándar b. Aprobado en 2003 para dar mayor velocidad con cierto grado de compatibilidad a equipamiento 802.11b.
- ✓ 802.11h. DFS: Dynamic Frequency Selection, habilita una cierta coexistencia con HiperLAN y regula también la potencia de difusión.
- ✓ 802.11i. Es un protocolo de seguridad (aprobada en Julio de 2004). Pretende reducir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado). Se implementa en WPA2.

Conceptos básicos

DEFINICIONES

Estandares Wifi

- ✓ 802.11j. Es equivalente al 802.11.h, pero en la regulación japonesa. Permite la armonización entre IEEE (802.11), ETSI (HiperLAN2) y ARIB (HISWANa).
- ✓ 802.11k. Mantenimiento redes wireless. Permite a los AP gestionar los recursos de radiofrecuencia asignados a los clientes.
- ✓ 802.11n. Mejora las versiones anteriores manteniendo la compatibilidad con ellas, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps. El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009. Permite trabajar en dos bandas de 2,4 y 5 GHz. Se prevé que el futuro estándar sustituto de 802.11n será 802.11ac con tasas de transferencia superiores a 1 Gb/s.4
- ✓ 802.11p. Este estándar opera en el espectro de frecuencias de 5,90 GHz y de 6,20 GHz, especialmente indicado para automóviles.

Conceptos básicos

DEFINICIONES

Estandares Wifi

- ✓ 802.11r. Se conoce como Fast Basic Service Set Transition, y su principal característica es permitir a la red que establezca los protocolos de seguridad que identifican a un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él. Permite que la transición entre nodos demore menos de 50 milisegundos. Un lapso de tiempo de esa magnitud es lo suficientemente corto como para mantener una comunicación vía VoIP sin que haya cortes perceptibles.

- ✓ 802.11w. Todavía no concluido. El grupo de trabajo IEEE 802.11w intenta extender la protección que aporta el estándar 802.11i más allá de los datos hasta las tramas de gestión, responsables de las principales operaciones de una red.

Conceptos básicos

DEFINICIONES

Tabla resumen de los estándares 802.11

ESTÁNDARES	AÑO RAFITIFACIÓN	VELOCIDAD TRANSMISIÓN	BANDA DE FRECUENCIA	PRINCIPAL INNOVACIÓN
802.11 Legacy	1997	1 Mbit/s – 2 Mbit/s	2,4 GHz	- CSMA/CA - Señales IR
802.11a	1999	20 Mbit/s – 54 Mbit/s	5 GHz	- Redes inal. - Banda 5 GHz
802.11b	1999	11 Mbit/s	2,4 GHz	- Banda 2,4 GHz - Soporte vel 5,5-11Mbit/s
802.11g	2003	54 Mbit/s	2,4 GHz	- Mayor Vtx - Compatible con 802.11b
802.11n	2004	600 Mbit/s	2,4 GHz y 5 GHz	- Mayor Vtx - Mayor alcance - Compat. 2 frec.

Conceptos básicos

Componentes de una red inalámbrica.

- **Tarjeta de red inalámbrica:** También denominada Adaptador Inalámbrico (AI) o WNIC (*Wireless Network Interface Card*), sirven para conectar un equipo a una red inalámbrica. En función del tipo del puerto de conexión que utilicen se dividen, fundamentalmente, en cuatro tipos: PCI, Mini PCI (para ordenadores portátiles), PCMCIA y USB.
- Las tarjetas PCI para Wi-Fi se agregan (o vienen de fábrica) a los ordenadores de sobremesa. Hoy en día están perdiendo terreno debido a las tarjetas USB. Dentro de este grupo también pueden agregarse las tarjetas MiniPCI que vienen integradas en casi cualquier computador portátil disponible hoy en el mercado.

Conceptos básicos

Componentes de una red inalámbrica.

- Las tarjetas PCMCIA son un modelo que se utilizó mucho en los primeros ordenadores portátiles, aunque están cayendo en desuso, debido a la integración de tarjeta inalámbricas internas en estos ordenadores. No permiten disfrutar de una velocidad de transmisión demasiado elevada

Conceptos básicos

Componentes de una red inalámbrica.

- Las tarjetas USB para Wi-Fi son el tipo de tarjeta más común que existe en las tiendas y más sencillo de conectar a un PC, ya sea de sobremesa o portátil, haciendo uso de todas las ventajas que tiene la tecnología USB. Hoy en día puede encontrarse incluso tarjetas USB con el estándar 802.11n (Wireless-N) El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 Ghz y 5 Ghz, que es el último estándar liberado para redes inalámbricas.
- También existen impresoras, cámaras Web y otros periféricos que funcionan con la tecnología Wi-Fi, permitiendo un ahorro de mucho cableado en las instalaciones de redes y especialmente, gran movilidad.

Conceptos básicos

DEFINICIONES

Cómo se realiza una conexión a una red inalámbrica

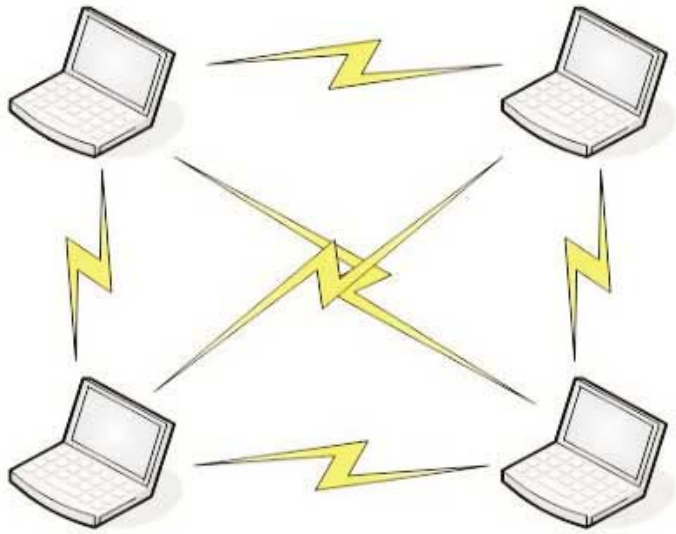
- Los puntos de acceso inalámbrico están constantemente emitiendo, en intervalos de tiempo fijos, "*beacon frames*" (balizas) para informar de su presencia. Si un cliente quiere asociarse con un AP y unirse a una red, ha de escuchar en busca de "*beacon frames*" para detectar los puntos de acceso que están a su alcance.
- Opcionalmente, puede enviar una trama denominada "*Prove Request*" que contenga un ESSID determinado para intentar localizar un punto de acceso concreto.

- Una vez identificado y seleccionado el AP, se realiza una autentificación del cliente mediante el intercambio de unas tramas de notificación denominadas "*management frames*". Si la verificación de la identidad es satisfactoria, el cliente ya está reconocido por los dispositivos de la red, pero aún no puede emitir datos ni participar de los recursos. Se dice, entonces, que está autenticado y disociado (o no asociado). Finalmente, el cliente se ha de asociar a un punto de acceso, que será responsable de la distribución de sus datos, para que pueda comunicarse con otros terminales de la red.

Conceptos básicos

MODO AD-HOC

Red wireless compuesta únicamente por estaciones con iguales derechos.
Esta topología se caracteriza por que no hay Punto de Acceso (AP), las estaciones se comunican directamente entre si (peer-to-peer), de esta manera el área de cobertura está limitada por el alcance de cada estación individual.
Las redes *peer-to-peer en general, no solo las wifi,* aprovechan, administran y optimizan el uso del ancho de banda de los demás usuarios de la red por medio de la conectividad entre los mismos, y obtienen así más rendimiento en las conexiones y transferencias que con algunos métodos centralizados convencionales, donde una cantidad relativamente pequeña de servidores provee el total del ancho de banda y recursos compartidos para un servicio o aplicación

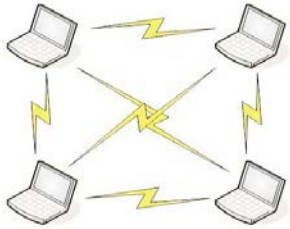


Conceptos básicos

MODO AD-HOC

- En redes de comunicación inalámbrica, una red ad hoc es aquella en la que no hay un nodo central, sino que todos los dispositivos están en igualdad de condiciones. Ad hoc es el modo más sencillo para el armado de una red. Sólo se necesita contar con 2 placas o tarjetas de red inalámbricas (de la misma tecnología). Una vez instaladas en los PC se utiliza el software de configuración del fabricante para configurarlas en el modo ad-hoc, definiendo el identificador común que utilizarán (SSID). Este modo es recomendable sólo en caso de que se necesite una comunicación entre no más de dos dispositivos.

- 802.11b también ofrece un modo ad hoc, en el que dos o más ordenadores intercambian datos directamente sin un punto de acceso central, algo muy parecido a los viejos tiempos en que se utilizaba un cable Ethernet cruzado o se enchufaba un cable de módem entre dos puertos en serie de dos ordenadores.



Conceptos básicos

MODO AD-HOC

- La diferencia entre el modo ad hoc y un punto de acceso de software o hardware es que las conexiones ad hoc no tienen un punto central de autoridad.
- Las conexiones ad hoc son completamente privadas entre las máquinas en cuestión.
- Dado que las conexiones ad hoc sólo existen entre dos o más ordenadores, son útiles principalmente para transferir archivos; si necesitamos dar un archivo a un colega y no tenemos otra forma de hacerlo, activar la opción de compartir archivos y establecer una red ad hoc bastará para llevar a cabo la tarea

<u>Algunos ejemplos de aplicación de las redes P2P son los siguientes:</u>

- Intercambio y búsqueda de ficheros. Quizás sea la aplicación más extendida de este tipo de redes. Algunos ejemplos son BitTorrent o la red eDonkey2000.
- Sistemas de ficheros distribuidos, como CFS o Freenet.
- Sistemas para proporcionar cierto grado de anonimato, como i2p, Tarzan o MorphMix. Son tecnologías que forman parte de la red oscura y constituyen el llamado peer-to-peer anónimo.
- Sistemas de telefonía por Internet, como Skype.
- A partir del año 2006, cada vez más compañías europeas y norteamericanas, como Warner Bros o la BBC, empezaron a ver el P2P como una alternativa a la distribución convencional de películas y programas de televisión, y ofrecen parte de sus contenidos a través de tecnologías como la de BitTorrent.9
- Cálculos científicos que procesen enormes bases de datos, como los procedimientos bioinformáticos.
- Monedas virtuales para transacciones entre partes. Bitcoin

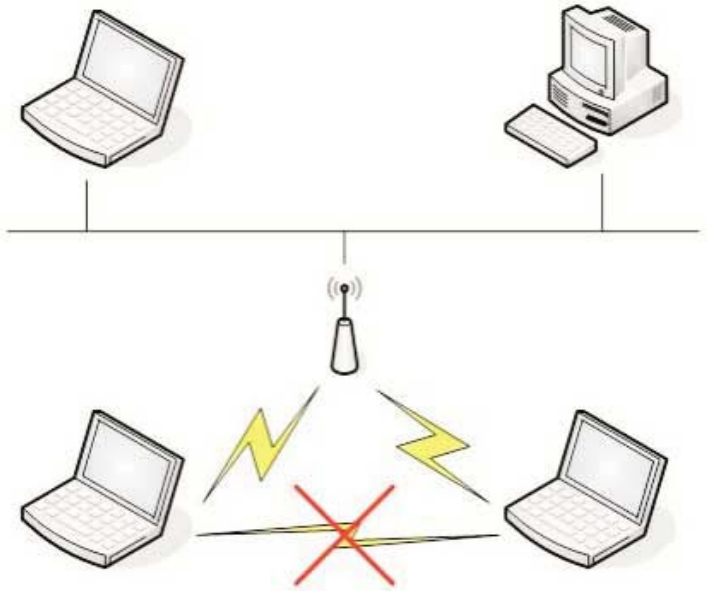
Conceptos básicos

MODO INFRAESTRUCTURA

En el modo Infraestructura como mínimo se dispone de un Punto de Acceso (AP) y las estaciones wireless no se pueden comunicar directamente, todos los datos deben pasar a través del AP. Todas las estaciones deben ser capaces de establecer conexión con el AP.

La mayoría de las redes wireless que podemos encontrar en las empresas utilizan modo infraestructura con uno o más Puntos de Acceso. El AP actúa como un HUB en una red cableada, redistribuye los datos hacia todas las estaciones.

Punto de Acceso (PA): Cualquier entidad que tiene funcionalidad de estación y provee acceso a servicios de distribución vía inalámbrica para estaciones asociadas.



SEGURIDAD EN REDES WIRELESS

REDES ABIERTAS

- Se caracterizan por no tener implementado ningún sistema de autentificación o cifrado. Las comunicaciones entre los AP y los terminales viajan sin cifrar. No se requiere ningún dato para acceder a la red.
- Los elementos que proporcionan seguridad a la red son:
  - Direcciones MAC
  - Direcciones IP
  - ESSID de la red
- La forma de filtrar el acceso a la red, es permitir al acceso solo a los terminales que tengan una dirección MAC o IP, o impidiendo el envío de los ESSID, de forma que solo se conecten los que conozcan el ESSID de la red.

- *Se alerta del creciente número de usuarios afectados por incidencias de seguridad en sus dispositivos móviles como consecuencia de su exposición a redes Wi-Fi abiertas sin las medidas de protección adecuadas.*
- *Además, existen estudios, ante el crecimiento de los usuarios que se conectan a redes Wi-Fi desde dispositivos móviles, que el número de infectados a través de este tipo de conexiones sigue creciendo de forma notable, sobre todo, aquellos que utilizan conexiones inalámbricas públicas y que muchos locales ofrecen gratuitamente, aunque sin las garantías necesarias para la protección de estos dispositivos.*

SEGURIDAD EN REDES WIRELESS

REDES ABIERTAS

- *Según estudios de Kaspersky Lab,*
  - *el 47% de los españoles utiliza redes Wi-Fi gratuitas abiertas desde sus smartphones*
  - *Un 45% accede desde tablets*
  - *Un 27% desde portátiles.*
  - *Sigue creciendo la asiduidad con la que los usuarios se conectan a este tipo de redes inalámbricas, muchos de los cuales lo hacen todo los días o, como mínimo, 2 o 3 veces por semana.*

- *Ante estos datos, los cibercriminales han puesto sus miras en estos usuarios a los que, en no pocas ocasiones, interceptan sus datos que quedan al descubierto en estas redes abiertas que no cuentan con contraseñas ni sistemas de cifrado adecuados.*

- *Ante estas cifras, se aconseja extremar las precauciones y disponer de soluciones de seguridad adecuadas que protejan a los usuarios de estas amenazas*

SOLUCIONES DE SEGURIDAD

FILTRADO DE DIRECCIONES MAC

Consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica.

Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta posee una dirección MAC única, se logra autentificar el equipo.

Este método tiene como ventaja su sencillez por lo cual se puede usar para redes caseras o pequeñas. Sin embargo posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

- No escala bien, porque cada vez que desee autorizar o dar de baja a un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso.
- Después de cierto numero de equipos o puntos de acceso, la situación se torna inmanejable.
- El formato de una dirección MAC no es amigable (normalmente se escriben con bytes en hexadecimal) lo que puede llevar a cometer errores en la manipulación de las listas y convertirse en un punto en contra desde el punto de vista de la seguridad.
- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar tarjetas MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computadora. De este modo, el atacante puede hacerse pasar por un cliente valido.

SOLUCIONES DE SEGURIDAD

FILTRADO DE DIRECCIONES MAC

- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un equipo que la red reconoce como válido. En el caso que el elemento robado sea un punto de acceso el problema se hace mas serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

El cifrado es prácticamente nulo.

Ventajas y desventajas con filtrado de direcciones MAC

Ventajas:

· Establece una seguridad media-baja ya que las tarjetas MAC pueden ser "clonadas".

· Gran sencillez para la administración de redes pequeñas o caseras.

Desventajas:

· No se puede asociar una dirección de MAC a un nombre de usuario, por lo que sólo se puede autenticar por identidad de equipo y no por identidad de usuario.

· Las direcciones MAC viajan sin cifrar por el aire y pueden ser capturadas empleando programas.

· El formato MAC no es amigable permitiendo errores de manipulación en las listas.

· No escala bien ya que se tiene que autorizar o dar de baja a un equipo manipulando las tablas de todos los puntos de acceso.

· En caso de extravío o robo de la tarjeta inalámbrica se compromete la seguridad de toda la red dando un tiempo prolongado hasta tomar las acciones debidas.

SEGURIDAD EN REDES WIRELESS

REDES ABIERTAS

MODOS DE ATAQUE

Romper ACL's {Access Control Lists} basados en MAC
Se basa en cambiar la dirección MAC del terminal atacante, e instalar una dirección MAC autorizada en la ACL

Ataque de Denegación de Servicio (DoS)
Se basa en impedir la comunicación entre un terminal y un AP, haciéndose pasar por el AP, una vez obtenido el MAC (obtenida mediante un sniffer) del AP, negarle la comunicación al terminal elegido mediante un envío continuado de denegación de servicio.
Otra forma de impedir la comunicación entre un terminal y un AP es interfiriendo la señal de radio, por ejemplo introduciendo una señal fuerte de ruido

Sniffer: Programa de captura de paquetes de red; El funcionamiento de un sniffer depende del estado en que se coloca la tarjeta de red: modo promiscuo o normal.
En modo promiscuo el sniffer captura todo el trafico de red, a diferencia del modo normal de funcionamiento que solamente intercepta el trafico saliente o entrante que corresponda a la tarjeta de red.

SEGURIDAD EN REDES WIRELESS

REDES ABIERTAS

MODOS DE ATAQUE

Descubrir ESSID ocultos

Si se bloquea a los AP para que no envíen constantemente los ESSID, se puede atacar de dos formas:

- Snifar la red hasta que algún terminal se conecte y obtener el ESSID
- Provocar la desconexión de algún terminal, con el método anterior, ataque DoS, pero sin mantenerlo desconectado.

Ataque Man in the Middle

Aparece como consecuencia de la aparición de los switches, que dificultan el empleo de sniffers para obtener datos.

Se basa en hacer creer a la víctima que el atacante es el AP, y al contrario.

Para realizar el ataque, es necesario obtener mediante sniffer:

- El ESSID de la red
- La dirección MAC del AP
- La dirección MAC de la víctima

Mediante el ataque DoS se rompe la conexión entre el cliente y el Ap. Cuando la tarjeta del cliente busca un nuevo AP, el atacante la suplanta y se hace pasar por el AP, poniendo su tarjeta en modo de trabajo Master.

También el atacante suplanta la identidad del cliente con el Ap, de forma que se coloca entre el cliente y el AP.

SEGURIDAD EN REDES WIRELESS

REDES ABIERTAS

MODOS DE ATAQUE

Ataque ARP Poisoning

Es una variante del Man in de Midle, mediante la alteración de la tabla ARP, (Address Resolution Protocol) (Protocolo de resolución de direcciones), que mantienen los dispositivos en red. El objetivo de este ataque consiste en acceder al contenido de la comunicación entre dos terminales conectados mediante dispositivos inteligentes como un switch. No es un ataque exclusivo de redes wifi.

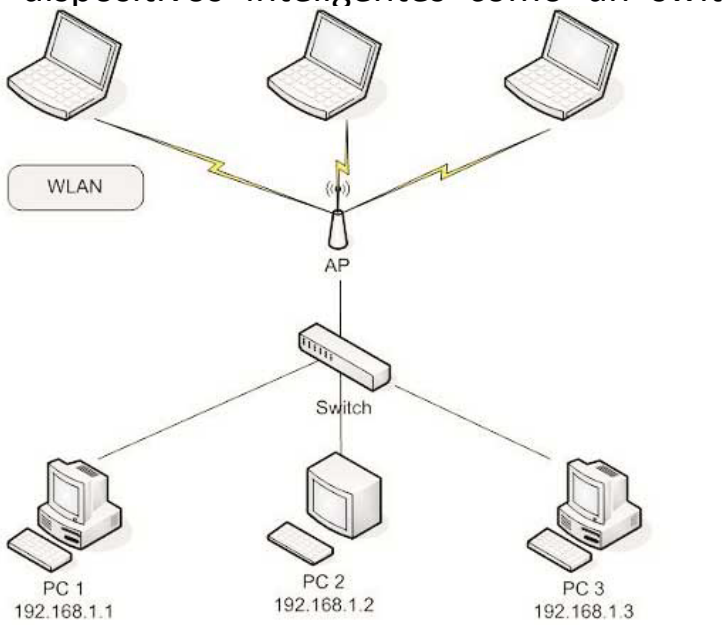


Tabla ARP -PC 1

Dirección IP	Dirección MAC
192.168.1.2	F2:F2:F2:F2:F2:F2
192.168.1.3	F3:F3:F3:F3:F3:F3

Tabla ARP -PC 2

Dirección IP	Dirección MAC
192.168.1.1	F1:F1:F1:F1:F1:F1
192.168.1.3	F3:F3:F3:F3:F3:F3

Tabla ARP -PC 3

Dirección IP	Dirección MAC
192.168.1.2	F2:F2:F2:F2:F2:F2
192.168.1.1	F1:F1:F1:F1:F1:F1

SEGURIDAD EN REDES WIRELESS

REDES ABIERTAS

MODOS DE ATAQUE

Ataque ARP Poisoning

El atacante envía paquetes ARP REPLY al PC3 diciendo que la dirección IP de PC 1 la tiene la MAC del atacante, de esta manera consigue modificar la caché de ARP's del PC 3. Luego realiza la misma operación atacando a PC 1 y haciéndole creer que la dirección IP de PC3 la tiene también su propia MAC.

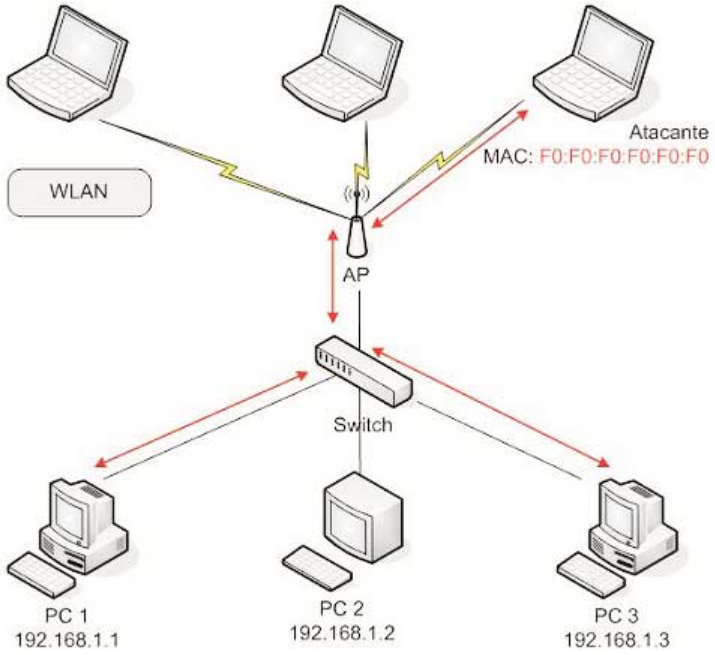


Tabla ARP -PC 1

Dirección IP	Dirección MAC
192.168.1.2	F2:F2:F2:F2:F2:F2
192.168.1.3	F0:F0:F0:F0:F0:F0

Tabla ARP -PC 2

Dirección IP	Dirección MAC
192.168.1.1	F1:F1:F1:F1:F1:F1
192.168.1.3	F3:F3:F3:F3:F3:F3

Tabla ARP -PC 3

Dirección IP	Dirección MAC
192.168.1.2	F2:F2:F2:F2:F2:F2
192.168.1.1	F0:F0:F0:F0:F0:F0

SEGURIDAD EN REDES WIRELESS

WEP (Wired Equivalent Privacy)

INTRODUCCIÓN

En las medidas de seguridad comentadas en la sección "Redes abiertas", en este tipo de sistemas todas las posibles medidas de seguridad que se pueden implantar se centran en intentar impedir la asociación a la red por parte de usuarios ilegítimos. En cambio ninguna de las medidas anteriores se empleaba para evitar la obtención de la información intercambiada entre terminales y AP (Contraseñas, etc...)

Para remediar esto se puede implementar el cifrado de las comunicaciones de tal forma que si alguien captura las comunicaciones entre los terminales y los AP, solo obtenga una serie de bytes sin sentido.

La idea es impedir la entrada a la red a intrusos, y si alguien entra en la red no pueda obtener información

SEGURIDAD EN REDES WIRELESS

WEP (Wired Equivalent Privacy)

PRINCIPIO DE FUNCIONAMIENTO

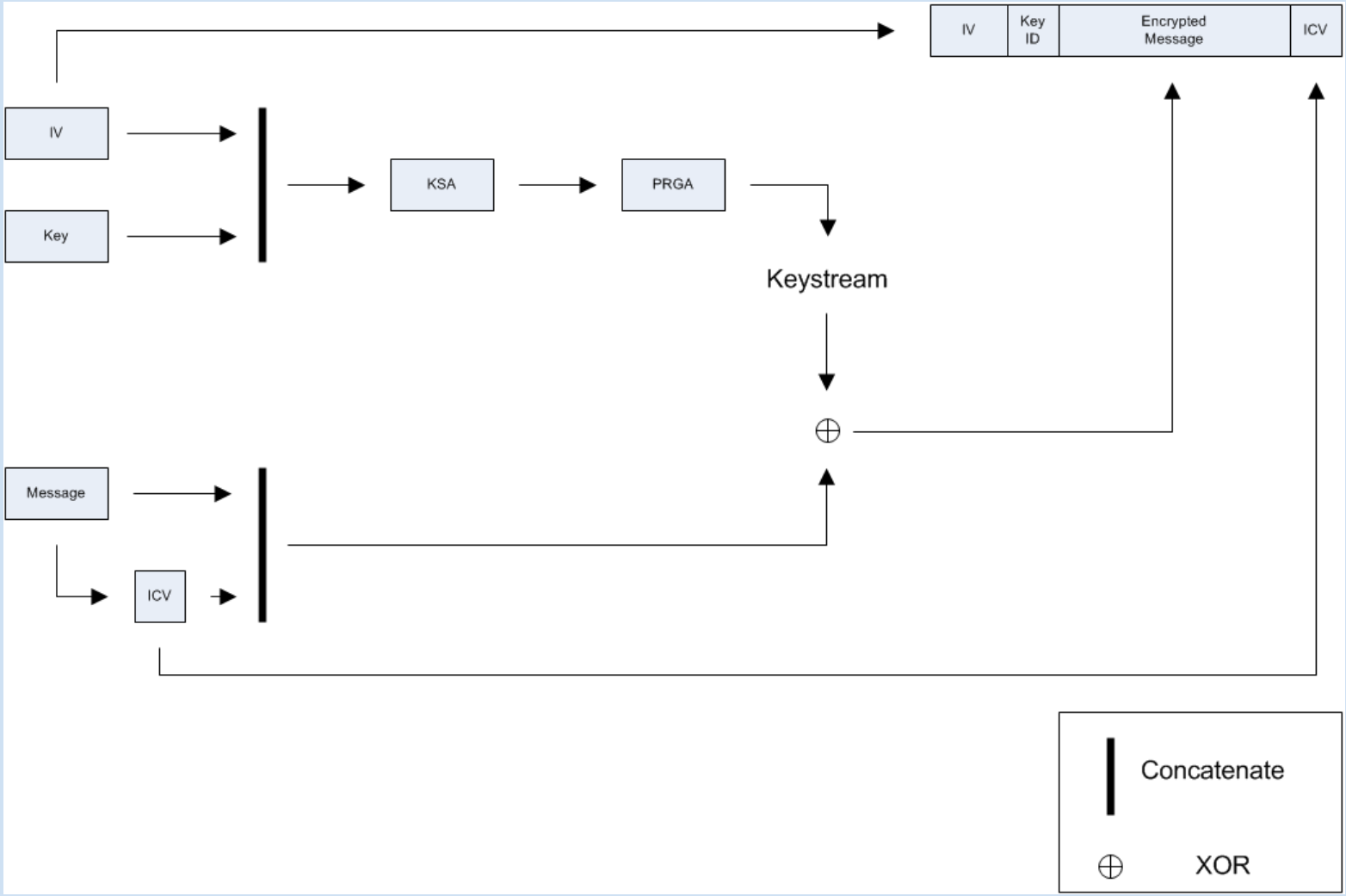
Es un algoritmo de protección de redes inalámbricas, realizado en la primera versión del estándar IEEE 802.11. Se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. Opera a nivel 2 (NIVEL DE ENLACE DE DATOS) del modelo OSI, y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

Emplea el algoritmo RC4 para el cifrado de llaves, de 64 o 128 bits. Tiene como pilar una clave secreta compartida por los comunicadores. Normalmente todas las estaciones y puntos de acceso comparten la misma clave, lo que reduce el nivel de seguridad del sistema.

Emplea un algoritmo de comprobación de integridad (CRC-32), que genera un ICV, que es un valor de comprobación de la integridad de los datos.

Este ICV, se añade al texto para comprobar que el mensaje no ha sido alterado.

WEP - Encriptación

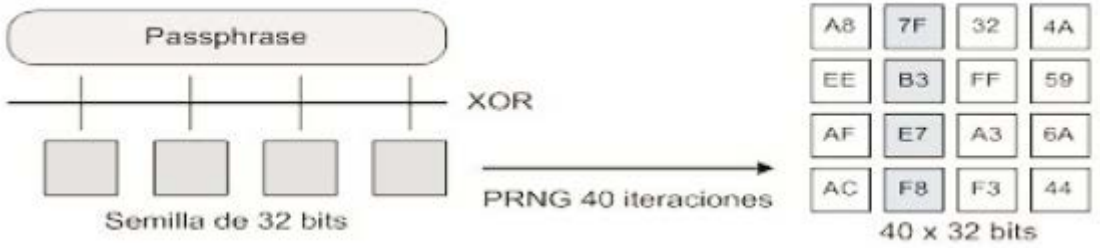


SEGURIDAD EN REDES WIRELESS

WEP (Wired Equivalent Privacy)

PRINCIPIO DE FUNCIONAMIENTO

LLAVES: A partir de la clave, normalmente sencilla, secreta para los comunicadores, se generan 4 llaves de 40 bits, de las que se empleará una diferente cada vez para realizar el cifrado WEP.
El proceso para obtener las llaves a partir de la clave consiste en la aplicación de una operación XOR con la cadena ASCII de la clave y de la cual se obtiene una semilla de 32 bits. Para realizar esta operación se divide la clave en grupos de 4 bytes de la siguiente manera:
Clave: "Mi clave WEP"
Se divide de esta forma:
M I _ C
L A V E
_ W E P
Y se realiza la operación XOR entre los elementos de cada columna; de esta manera obtenemos la semilla de 32 bits. Esta semilla es la que emplea un generador de numeros pseudoaleatorios (GNSA) para generar 40 cadenas de 32 bits cada una. A partir de un bit de cada una de las 40 cadenas se obtienen 4 llaves de 40 bits y (en cada ocasión) una de ellas se usara para realizar el cifrado WEP.



SEGURIDAD EN REDES WIRELESS

WEP (Wired Equivalent Privacy)

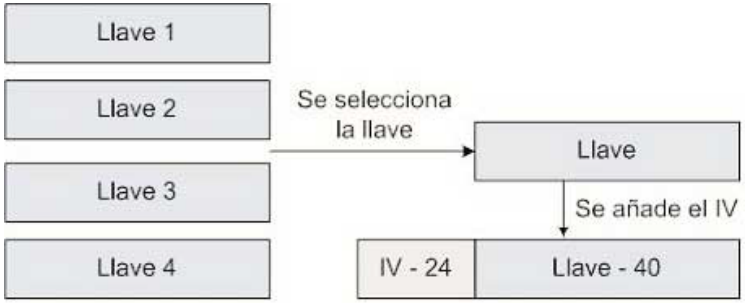
PRINCIPIO DE FUNCIONAMIENTO

CIFRADO: Las tramas se componen de una cabecera (Header) y un contenido (payload).

Trama 802.11

Pasos:

- Se calcula el CRC de 32 bits del payload (Texto) y se obtiene el ICV(Integrity Check Value) que se añadirá a la trama cifrada.
- Se genera la semilla: Se selecciona una de las llaves de 40 bits de entre las 4 posibles y se añade al Vector de Inicialización (IV). El IV es simplemente un contador que va cambiando de valor a medida que se generan tramas de forma que, al añadirlo a la llave, se aumenta el número de "llaves" posibles a emplear.

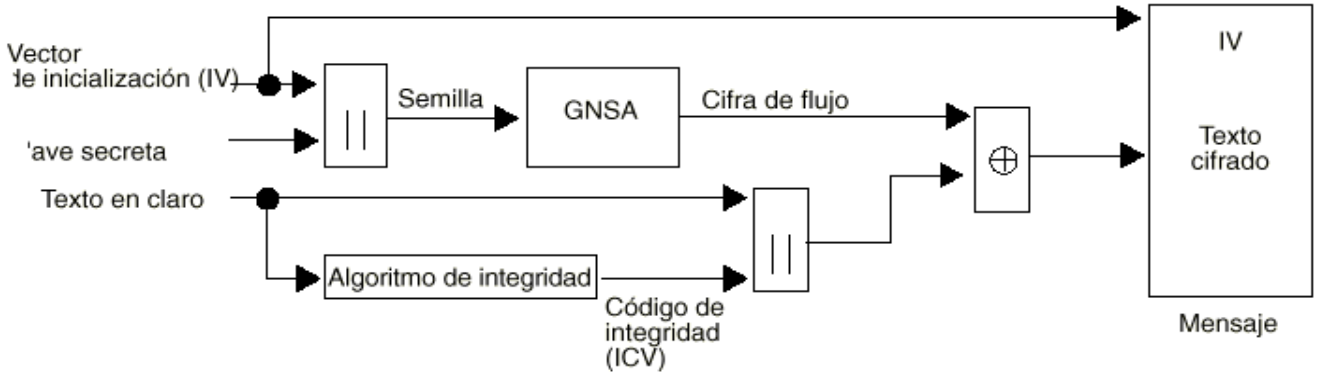


SEMILLA

SOLUCIONES DE SEGURIDAD

WEP (WIRED EQUIVALENT PRIVACY)

MODO TRANSMISOR:

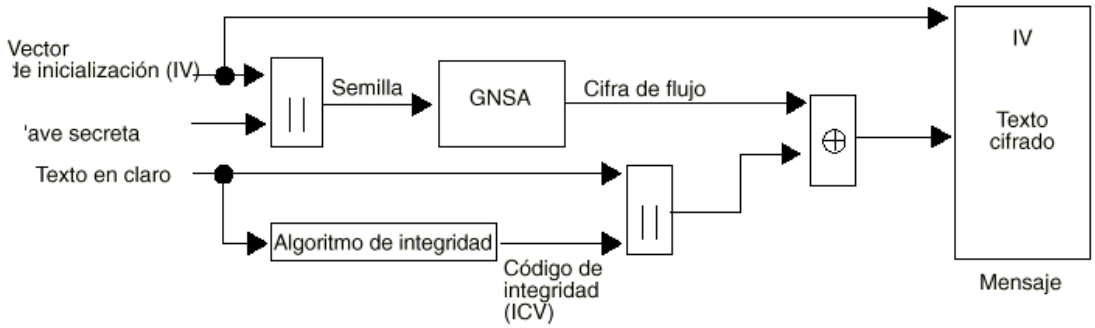


- Al texto a trasmitir se le realiza un algoritmo CRC-32 y genera un código de integridad (Integrity Check Value, ICV). Dicho ICV se concatena con la trama, y es empleado mas tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.
- Se generan 4 llaves de 40 bits a partir de la clave secreta compartida entre emisor y receptor, esta clave puede poseer 40 o 128 bits.
- Se escoge una llave de las 4, distinta cada vez.
- Se concatena la llave con un número aleatorio llamado vector de inicialización (IV) de 24 bits. El IV cambia con cada trama. En realidad es un contador de tramas. Se genera la semilla.
- La concatenación de la clave secreta y el IV (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo aleatorios (GNSA). El generador RC4 es capaz de generar una secuencia seudo aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.

SOLUCIONES DE SEGURIDAD

WEP (WIRED EQUIVALENT PRIVACY)

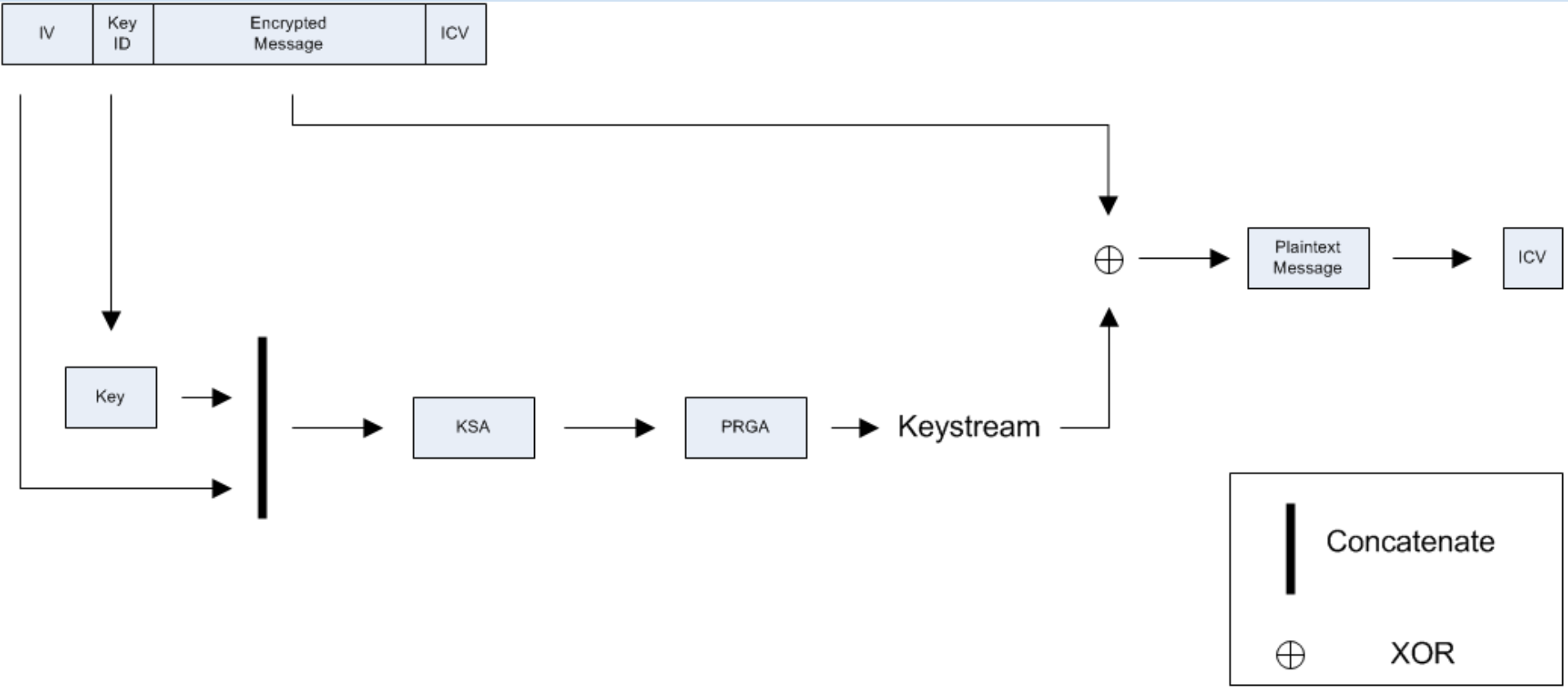
ESQUEMA MODO TRANSMISOR :



- El generador RC4 genera una cifra de flujo del mismo tamaño a la trama a cifrar mas 32 bits (para cubrir la longitud de la trama y el ICV).
- Se hace un XOR bit por bit de la trama con la secuencia de clave obteniéndose como resultado la trama cifrada.
- El IV y la trama se transmiten juntos.

- Tras esto se añade al conjunto [Enc. Payload + Enc. ICV] la cabecera de la trama y el IV, y se obtiene el paquete listo para ser enviado

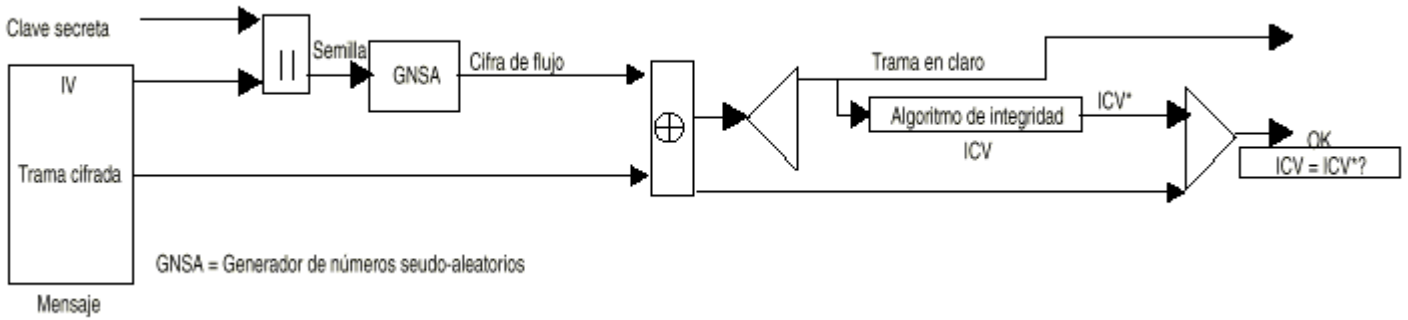
WEP - Desencriptar



SOLUCIONES DE SEGURIDAD

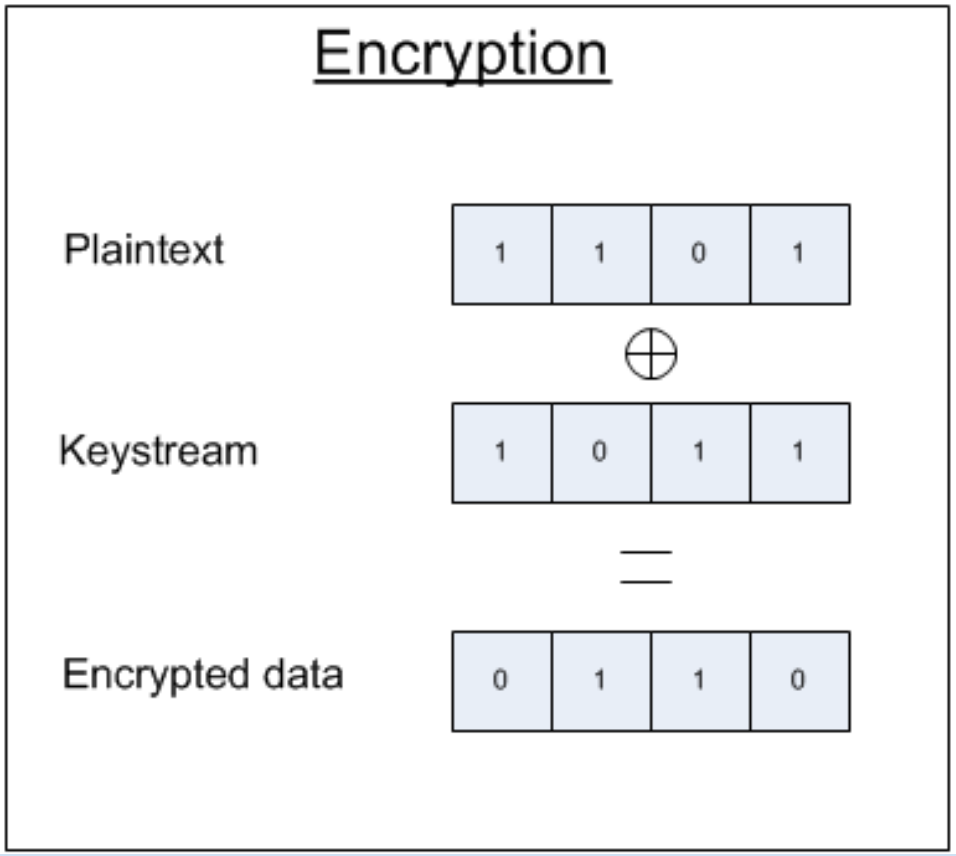
WEP (WIRED EQUIVALENT PRIVACY)

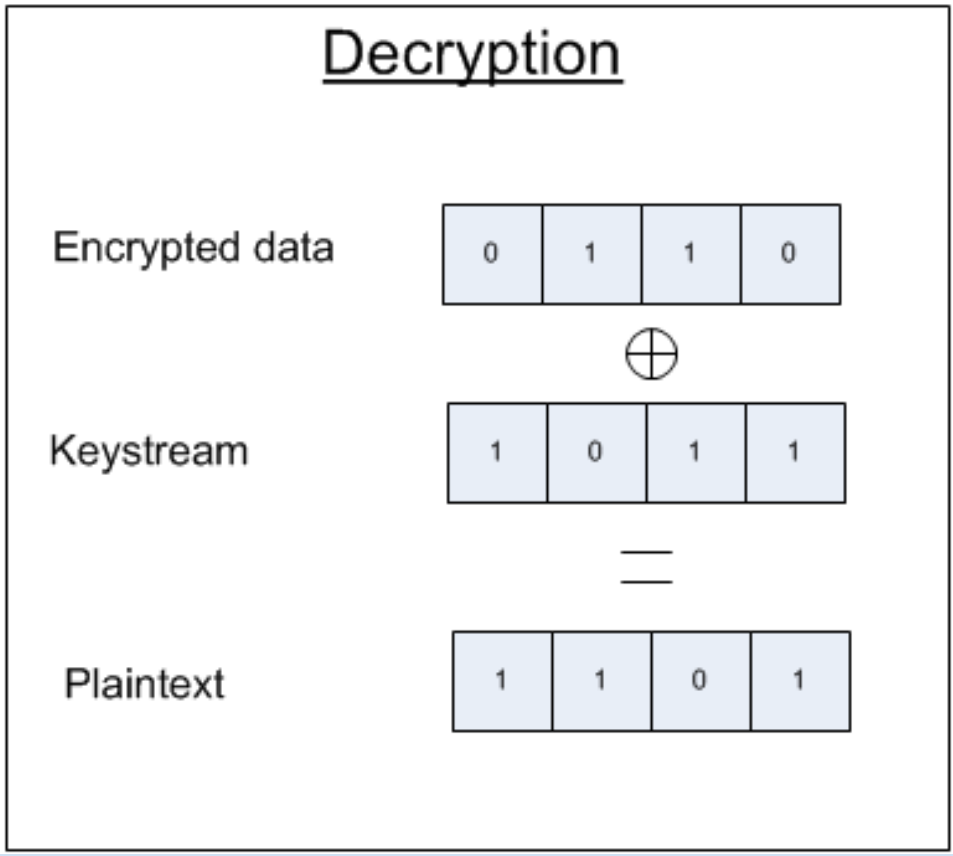
ESQUEMA MODO RECEPTOR:



- En el receptor se lleva a cabo el procedimiento de descifrado.
- Se emplea el IV recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.
- Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será la usada en la transmisión.
- Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrada, obteniéndose de esta manera la trama en claro y el ICV.
- A la trama en claro se le aplica el algoritmo CRC-32 para obtener un segundo ICV que se compara con el recibido.
- Si los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

Network Interaction – WEP-IV idéntico





SOLUCIONES DE SEGURIDAD

WEP (WIRED EQUIVALENT PRIVACY)

RESUMEN:

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre el emisor y el receptor.

Existen dos situaciones que hacen que WEP no sea seguro:

- La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca o muy de vez en cuando).
- El IV que se utiliza es de longitud insuficiente (24 bits). Dado que cada trama se cifra con un IV diferente, solamente es cuestión de tiempo para que se agote el espacio de 2^{24} IV distintos. No es problemático en una red casera con bajo tráfico, pero en una red que posea alto tráfico se puede agotar el espacio de los IV.

Si el atacante logra conseguir dos tramas con IV idéntico, puede efectuar un XOR entre ellas y obtener los textos en claro de ambas tramas mediante un ataque estadístico. Con el texto en claro de una trama y su respectivo texto cifrado se puede obtener la cifra de flujo, conociendo el funcionamiento del algoritmo RC4, es posible entonces obtener la clave secreta y descifrar toda la conversación.

SEGURIDAD EN REDES WIRELESS

WPA (Wi-Fi Protected Access)

PRINCIPIO DE FUNCIONAMIENTO

Modos de funcionamiento de WPA

WPA puede funcionar en dos modos:

- Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.

- Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

SOLUCIONES DE SEGURIDAD

WPA

- WPA (Wi-Fi Protected Access) es una revisión del cifrado WEP que se implementó con el estándar 802.11i. Fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario.

- Es un protocolo de control de acceso y autentificación basado en la arquitectura cliente servidor que restringe la conexión de equipos no autorizados a una red.

- El protocolo fue inicialmente creado por la IEEE para uso en redes de área local cableadas, pero se ha extendido también en las redes inalámbricas. Corrige las deficiencias de la seguridad WEP.

- WPA involucra dos aspectos: un sistema de encriptación mediante TKIP y un proceso de autentificación mediante 802.1x.

SOLUCIONES DE SEGURIDAD

WPA

❖ **SISTEMA DE ENCRIPTACIÓN TKIP**

– TKIP (Temporal Key Integrity Protocol), es el elegido como solución WEP. Es similar al WEP, con varias mejoras:

- Amplía la clave a 128 bits, y la hace dinámica. WPA automáticamente genera nuevas llaves de encriptación únicas para cada uno de los clientes, sesión y paquetes lo que evita que la misma clave se utilice durante semanas.

- El vector de inicialización (IV)pasa de 24 a 48 bits, lo que reduce significativamente la reutilización y por tanto la posibilidad de que un hacker recoja suficiente información para romper la encriptación.

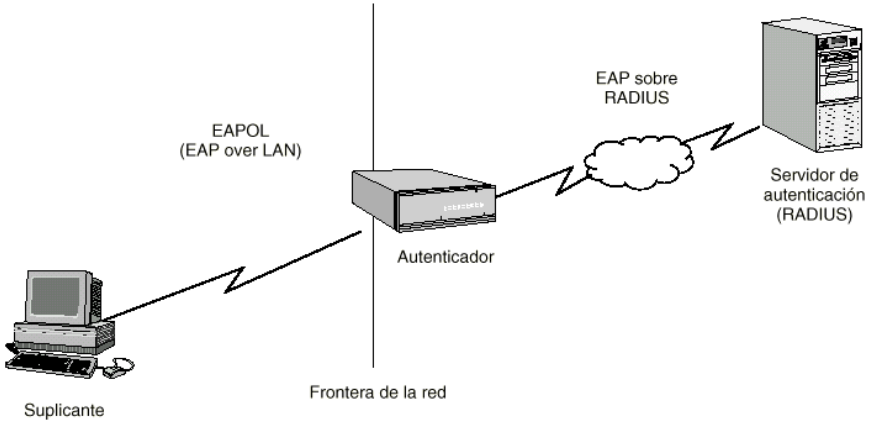
- Utiliza el algoritmo Michel para garantizar la integridad de los datos , genera un bloque de 4 bits (MIC) a partir de la dirección MAC de origen, destino y de los datos, y lo añade a los datos a enviar. Los datos a enviar se fragmentan y se les asigna un número de secuencia. La mezcla del número de secuencia con la clave temporal, genera la clave que se usa para el cifrado de cada fragmento.

SOLUCIONES DE SEGURIDAD

WPA

❖ **PROCESO DE AUTENTIFICACIÓN, MEDIANTE 802.1X/EAP**

- Incluye tres partes:
- El cliente que desea conectarse con la red.
- El servidor de autorización y autentificación que contiene toda la información necesaria para saber cuales equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS(Remote Authentication Dial In User Service).
- El autentificador que es el equipo de red (AP, enrutador, servidor de acceso remoto) que recibe la conexión del suplicante. El autentificador actúa como intermediario entre el cliente y el servidor de autenticación y solamente permite el acceso del suplicante a la red cuando el servidor así lo autoriza.



SOLUCIONES DE SEGURIDAD

WPA

PROCESO DE AUTENTIFICACIÓN

El protocolo EAP(Extensible Authentication Protocol), es una autenticación usada habitualmente en redes WLAN Point-to-Point Protocol. Aunque el protocolo EAP no está limitado a LAN inalámbricas y puede ser usado para autenticación en redes cableadas, es más frecuentemente su uso en las primeras. Recientemente los estándares WPA y WPA2 han adoptado cinco tipos de EAP como sus mecanismos oficiales de autenticación .

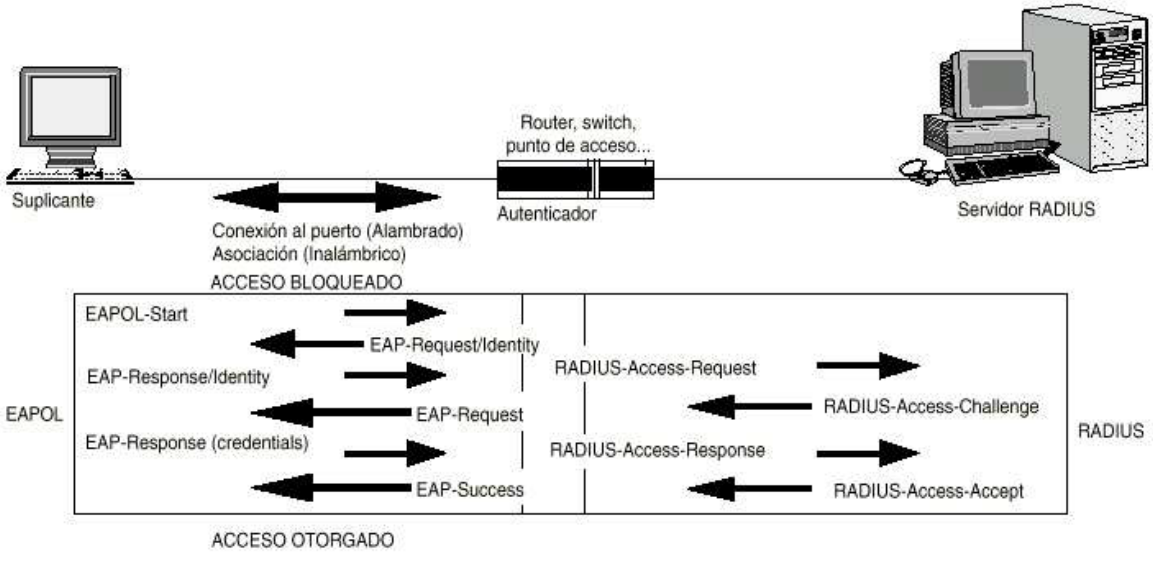
SOLUCIONES DE SEGURIDAD

WPA

PROCESO DE AUTENTIFICACIÓN

La autentificación del cliente se lleva a cabo mediante el protocolo EAP(Extensible Authentication Protocol y el servicio RADIUS de la siguiente manera:

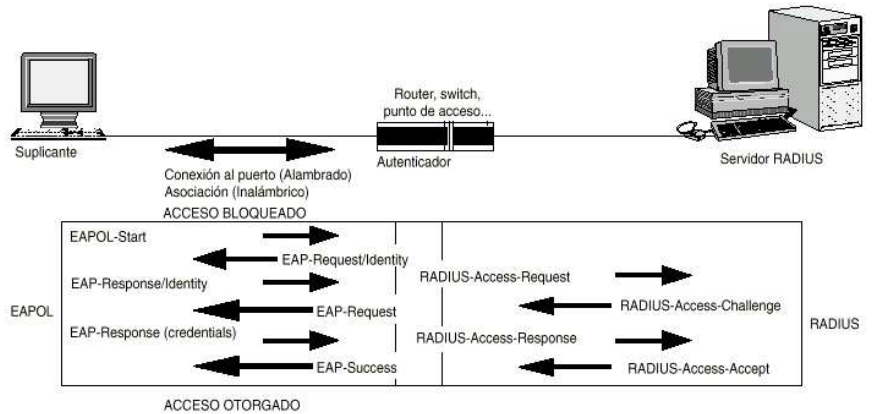
- Usuario intenta conectarse a la red, y activa su interfaz de red o logra enlazarse con un punto de acceso. Inicialmente la interfaz de red tiene el acceso bloqueado para el trafico normal y lo único que admite es el trafico EAP, que es requerido para efectuar la autentificación. El usuario envía un mensaje EAP–Start al autentificador indicando que desea iniciar el proceso de autentificación.
- El autentificador solicita a la estación que se identifique mediante un EAP Request/Identity.
- El usuario se identifica mediante un EAP Response/Identity.



SOLUCIONES DE SEGURIDAD

WPA

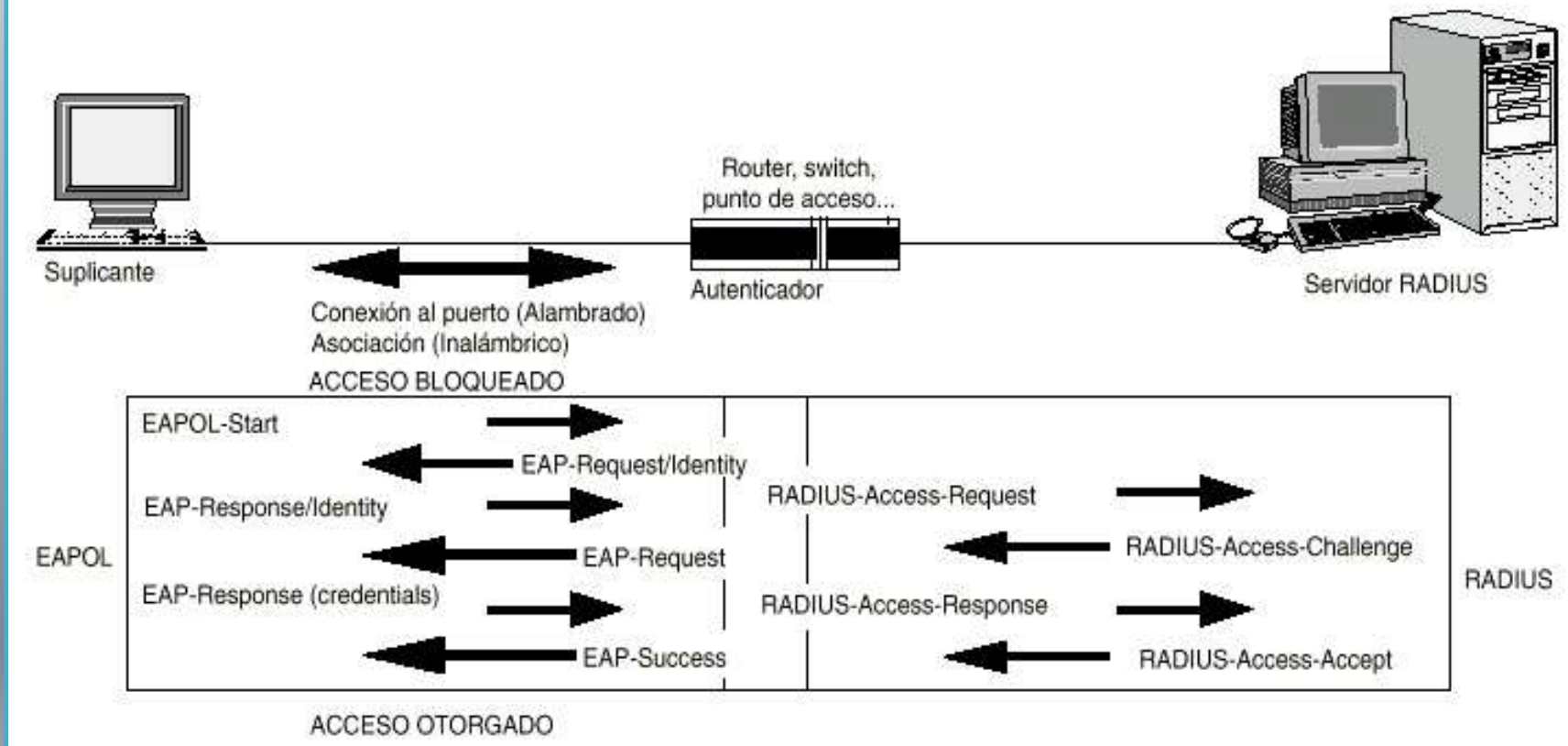
- Una vez recibida la información de identidad el autenticador envía un mensaje RADIUS–Access-Challenge, en el cual se envía información de un desafío que debe ser resuelto correctamente por el usuario para lograr el acceso. Dicho desafío puede ser tan sencillo como una contraseña o involucrar una función criptográfica más elaborada. El autentificador envía el desafío al cliente en un mensaje EAP/Request.
- El usuario da respuesta al desafío mediante un mensaje EAP/Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-Access-Response. Si toda la información de autentificación es correcta el servidor envía al autentificador un mensaje RADIUS Access Accept que autoriza al autentificador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red. En este mensaje se incluyen un juego de claves WEP dinámicas, que se usarán para cifrar la conexión entre el cliente y el punto de acceso. El servidor RADIUS se encarga de cambiar esta clave dinámica periódicamente para evitar obtenciones de clave.
- El autenticador envía un mensaje EAP-Success al cliente y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.



SOLUCIONES DE SEGURIDAD

WPA

Esquema de lo anterior:



SEGURIDAD EN REDES WIRELESS

WPA (Wi-Fi Protected Access)

RESUMEN

AUTENTIFICACIÓN MEDIANTE 802.1X/EAP

EL Protocolo de Autentificación Extensible (EAP) autentifica mediante:

Define 3 entidades:

- El solicitante, (Supplicant), está en el terminal
- El autenticador (Authenticator), está en el AP
- El servidor de autenticación, está en un servidor AAA(Authentication, Authorization, Accoounting), RADIUS

EAP UTILIZA cuatro tipos de mensajes:

- ❖Petición (Request Identity): Desde el AP al cliente.
- ❖Respuesta (Identity Response): Desde el cliente al AP.
- ❖Éxito (Success): emitido por el AP. El acceso está permitido.
- ❖Fallo (Failure): emitido por el AP. Se deniega la conexión.

Proceso de autenticación:

- ✓El Autenticador envía el EAP-Request/Identity al Suplicante.
- ✓El Suplicante responde con EAP-Response/Identity al Autenticador, el cual lo pasa al Servidor de Autenticación.
- ✓Si resulta acertado el Autenticador permite al Suplicante acceso a la red.

SOLUCIONES DE SEGURIDAD

WPA

Existen varias variantes del protocolo EAP según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad y las que utilizan contraseñas.

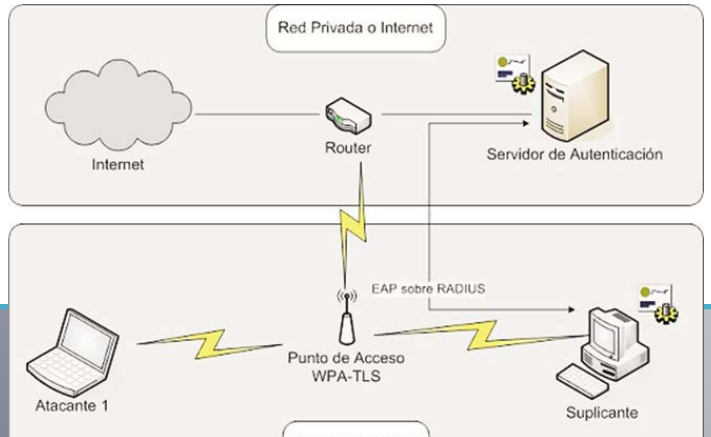
Las variantes de EAP que emplean certificados de seguridad son las siguientes:

EAP-TLS(Extensible Authentication Protocol-Transport Layer Security):

Requiere de instalación de certificados en los clientes y en el servidor.

Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. En el proceso de autenticación el solicitante envía su identificación (nombre de usuario) hacia el servidor de autenticación. El servidor envía su certificado al solicitante que, tras validarlo, responde con el suyo. Si el certificado del solicitante es válido, el servidor responde con el nombre de usuario antes enviado y se comienza la generación de la clave de cifrado, la cual es enviada al AP por el servidor de autenticación para que pueda comenzar la comunicación segura.

La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transport Layer substrate).



SEGURIDAD EN REDES WIRELESS

WPA

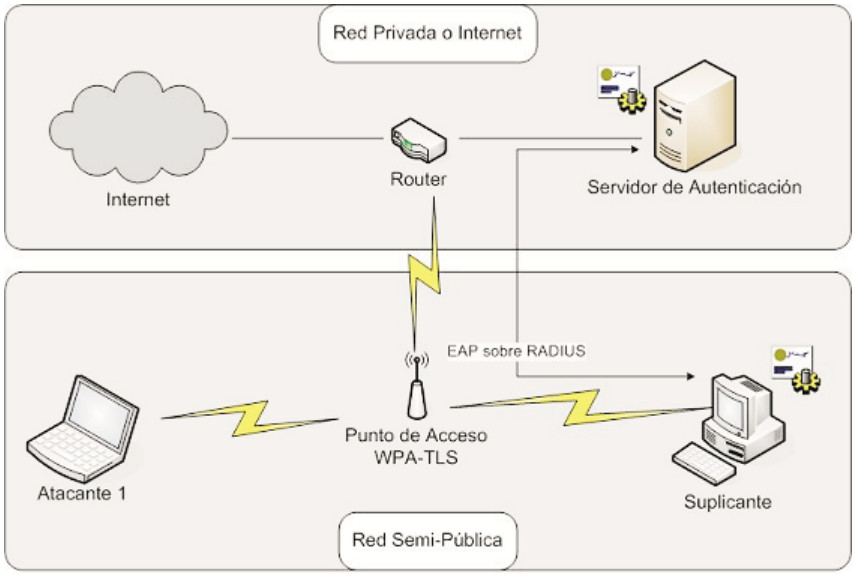
PRINCIPIO DE FUNCIONAMIENTO

EAP-TLS

Vulnerabilidad de la red.

En la fase de identificación el cliente manda el mensaje EAP-Identity sin cifrar, permitiendo a un atacante ver la identidad del cliente que está tratando de conectarse.

De la misma forma el envío de la aceptación/denegación de la conexión se realiza sin cifrar, con lo que un eventual atacante puede reenviar este tipo de tráfico para generar ataques de tipo DoS.



SOLUCIONES DE SEGURIDAD

WPA

PEAP y EAP-TTLS

El mayor inconveniente que tiene el uso de EAP-TLS es que tanto el servidor de autenticación como los clientes han de poseer su propio certificado digital, y la distribución entre un gran número de ellos puede ser difícil y costosa. Para corregir este defecto se crearon PEAP (Protected EAP) y EAP - Tunneled TLS que únicamente requieren certificado en el servidor.

La idea base de estos sistemas es que, empleando el certificado del servidor previamente validado, el cliente pueda enviar sus datos de autenticación cifrados a través de un túnel seguro. A partir de ese momento, y tras validar el servidor al solicitante, ambos pueden generar una clave de sesión.

SOLUCIONES DE SEGURIDAD

WPA

EAP-TTLS:

Desarrollada por Funk Software y Certicom.

Proporciona servicios similares a EAP-TLS, con la diferencia de que requiere solamente la instalación de un certificado en el servidor.

Esto garantiza la autenticación fuerte del servidor por parte del cliente; la autenticación del cliente por parte del servidor se efectúa una vez que se establece la sesión TLS, utilizando otro método tal como PAP, CHAP, MS-CHAP ó MS-CHAP v2.

PEAP:

Desarrollado por Microsoft, Cisco y RSA Security.

Funciona de manera parecida a EAP-TTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

SOLUCIONES DE SEGURIDAD

WPA

El empleo de certificados permite una autenticación fuerte entre cliente y servidor, sin embargo posee también varias desventajas:

- La administración de los certificados de seguridad puede ser costosa y complicada, especialmente en los esquemas donde se necesitan certificados en los clientes y en el servidor. Es necesario comprar los certificados a una autoridad de certificación (CA) conocida, o montar una CA propia.
- El diálogo de autenticación es largo. Esto ocasiona que el proceso sea algo demorado, siendo especialmente molesto para usuarios que tienen que reautenticarse con mucha frecuencia (por ejemplo, usuarios en movimiento que cambien de un punto de acceso a otro).
- La manipulación del certificado puede ser engorrosa para el usuario. En muchos casos se elige instalar el certificado en la terminal del usuario, con lo cual, si la terminal es robada y el certificado es el único nivel de seguridad que se posee, la seguridad de la red estaría en riesgo. Otra solución sería llevar el certificado en una tarjeta inteligente lo que obligaría a instalar hardware adicional.

SOLUCIONES DE SEGURIDAD

WPA

Las variantes de EAP que emplean contraseñas son las siguientes:

EAP-MD5:

Emplea un nombre de usuario y una contraseña para la autenticación.

La contraseña se transmite cifrada con el algoritmo MD5.

Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente).

Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada), y el esquema no es capaz de generar claves WEP dinámicas.

Por estos problemas, EAP-MD5 ha caído en desuso.

LEAP:

Esta variante es propietaria de Cisco.

Emplea un esquema de nombre de usuario y contraseña, y soporta claves dinámicas WEP. Al ser una tecnología propietaria, exige que todos los puntos de acceso sean marca Cisco, y que el servidor RADIUS sea compatible con LEAP.

SOLUCIONES DE SEGURIDAD

WPA

CUADRO COMPARATIVO A NIVEL DE SOLUCIONES 802.1X/EAP

Tema	EAP-MD5	LEAP (Cisco)	EAP-TLS (MS)	EAP-TTLS (Funk)	EAP-PEAP
Solución de Seguridad	Estándar	Patente	Estándar	Estándar	Estándar
Certificados-Cliente	No	N/A	Sí	No (opcional)	No (opcional)
Certificados-Servidor	No	N/A	Sí	Sí	Sí
Credenciales de Seguridad	Ninguna	Deficiente	Buena	Buena	Buena
Soporta Autenticación de Base de Datos	Requiere Borrar la Base de Datos	Active Directory, NT Domains	Active Directory	Act. Dir., NT Domains, Token Systems, SQL, LDAP	Active Directory
Intercambio de llaves dinámicas	No	Sí	Sí	Sí	Sí
Autenticación Mútua	No	Sí	Sí	Sí	Sí

SOLUCIONES DE SEGURIDAD

WPA

Ventajas y desventajas .

Ventajas:

- Se basa en un servidor de autenticación.
- El RADIUS realizará el juego de claves WEP.
- Existen protocolos de autenticación mutua entre cliente y servidor.

Desventajas:

- El empleo de certificados puede ser costoso.
- Generalmente es empleado para empresas grandes por su complejidad.
- La manipulación de los certificados lo hace engorrosa
- Existen protocolos que son débiles frente a ataques de “fuerza bruta” o de diccionario.

SEGURIDAD EN REDES WIRELESS

WPA (Wi-Fi Protected Access) - PSK

WPA y Seguridad en Pequeñas Oficinas - WPA-PSK (pre-shared key)
EAP necesita de un servidor RADIUS, lo que limita su implementación en redes pequeñas.

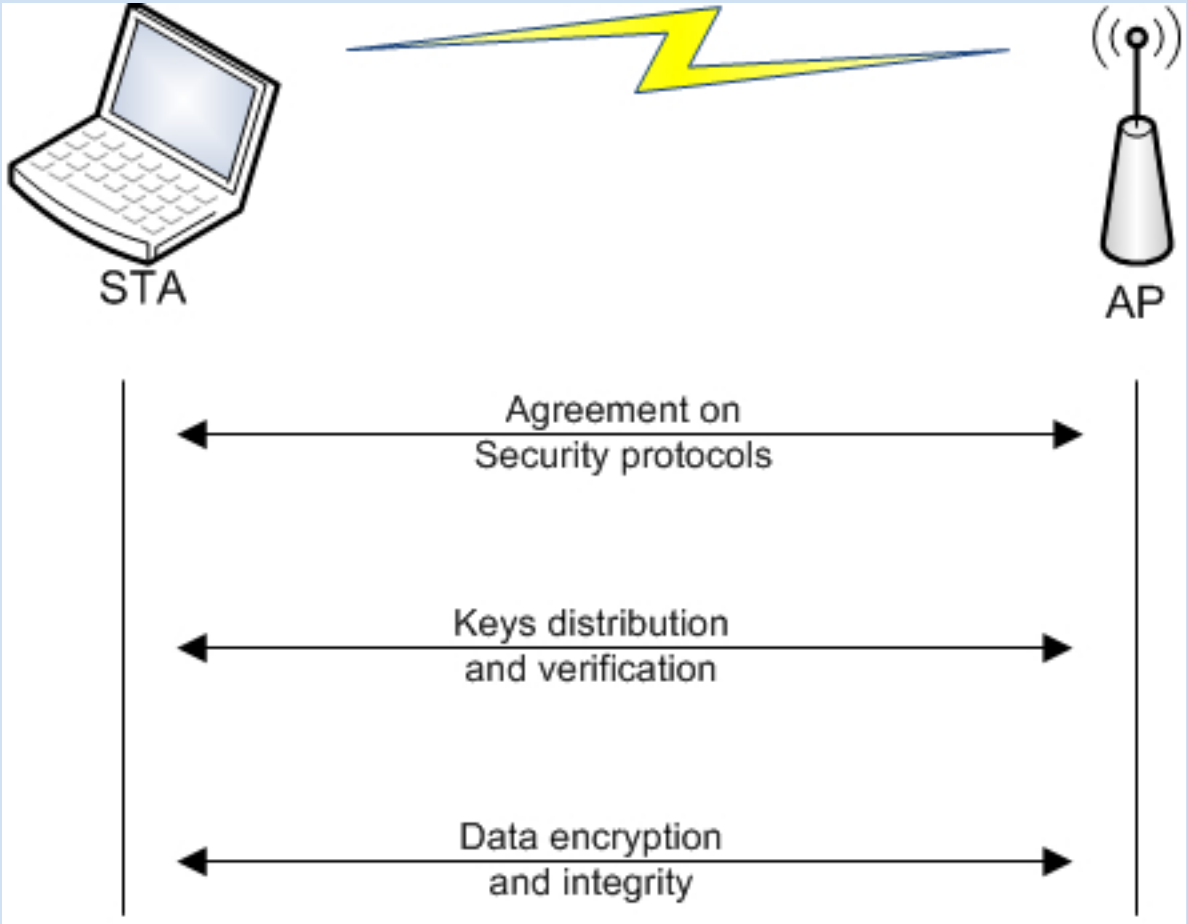
Se trata de ofrecer la seguridad Wi-Fi con los beneficios de WPA, mediante el uso de una clave pre-compartida (PSK, pre-shared key) o contraseña.

Permite el uso de TKIP (Proceso encriptación), pero configurando manualmente una clave en el cliente wireless y en el punto de acceso.

El estándar permite claves de hasta 256 bits, lo que proporciona una seguridad muy elevada. Sin embargo el escoger claves sencillas y cortas puede hacer vulnerable el sistema frente a ataques de fuerza bruta o diccionario.

Ataque WPA-PSK
El único ataque conocido contra WPA-PSK es del tipo fuerza bruta o diccionario; pese a la existencia de este ataque la realidad es que el rendimiento del ataque es tan bajo y la longitud de la passphrase puede ser tan larga, que implementarlo de forma efectiva es prácticamente imposible.

Network Interaction – WPA PSK



SEGURIDAD EN REDES WIRELESS

WPA (Wi-Fi Protected Access) - PSK

WPA-PSK (pre-shared key)

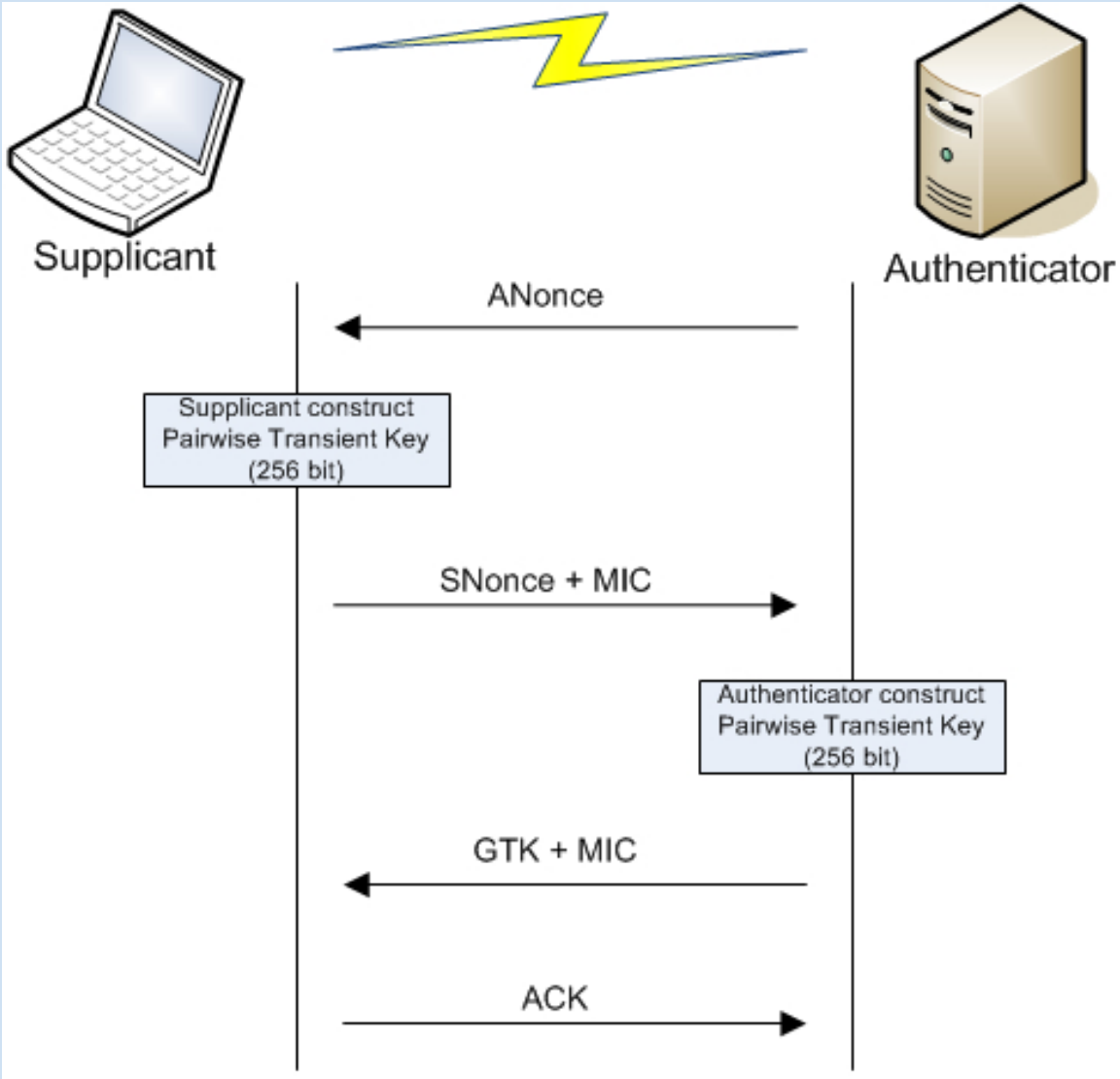
De un modo similar al WEP, el método PSK requiere introducir la misma clave compartida en todos los equipos de la red.

La clave PSK no es la cadena utilizada para encriptar los datos. A partir de la PSK se construye la PMK (Primary Master Key), que es lo que autentifica la estación ante el AP.

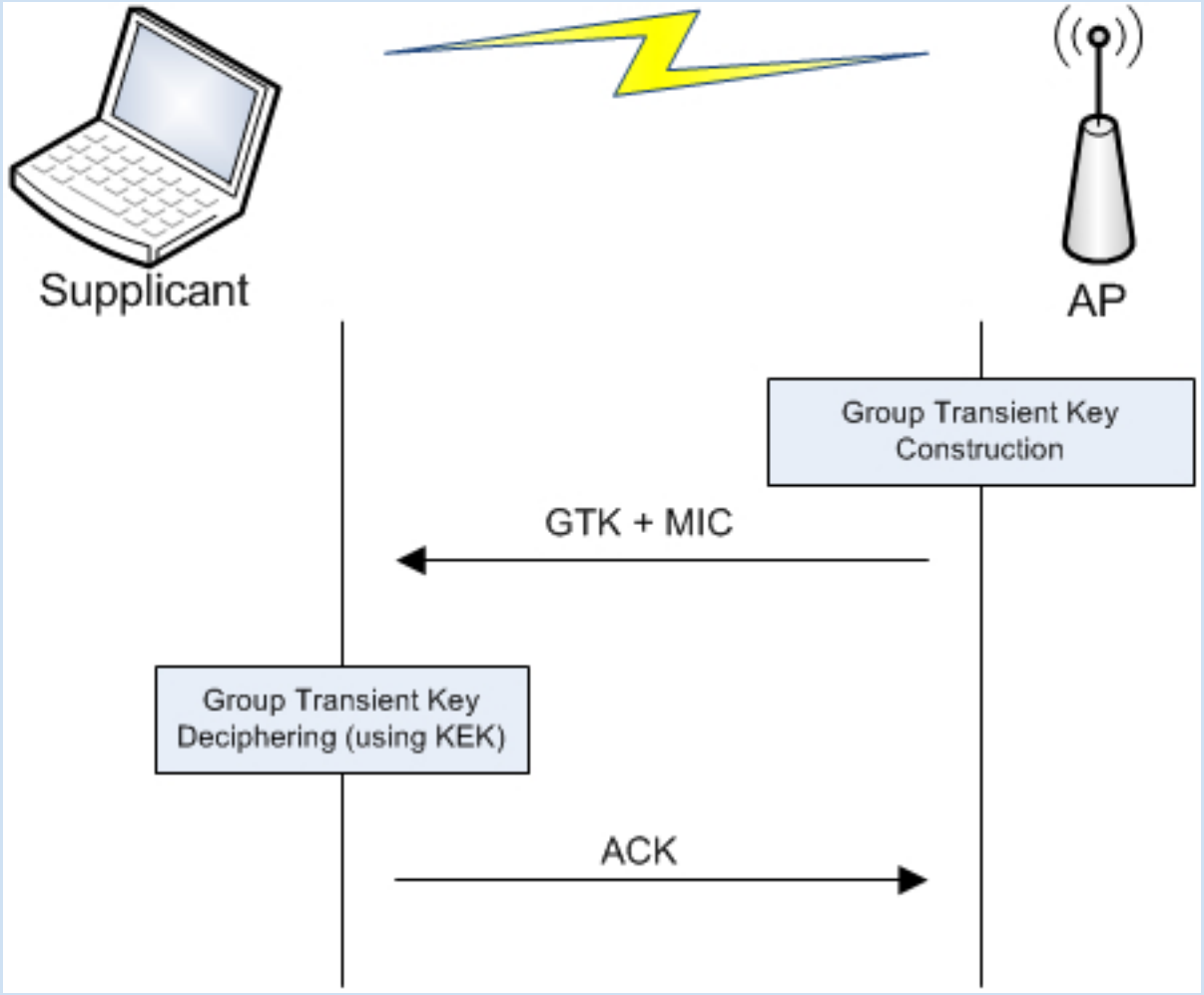
Con la PSK se genera, a través del intercambio de dos números aleatorios entre AP y cliente, una clave de cifrado para cada proceso de autenticación dependiendo del tráfico al que pertenece el paquete (unicast, Brodcast o multicast) llamada PTK (Primary Temporal Key) para el primero y GTK (Group Temporal Key) para los dos restantes.

Una vez el cliente está autenticado, el protocolo TKIP utiliza 6 claves de cifrado por cada sesión (4 de ellas para comunicaciones unicast y 2 broadcast) que son generadas a partir de las direcciones MAC, ESSID y la PTK antes mencionada.

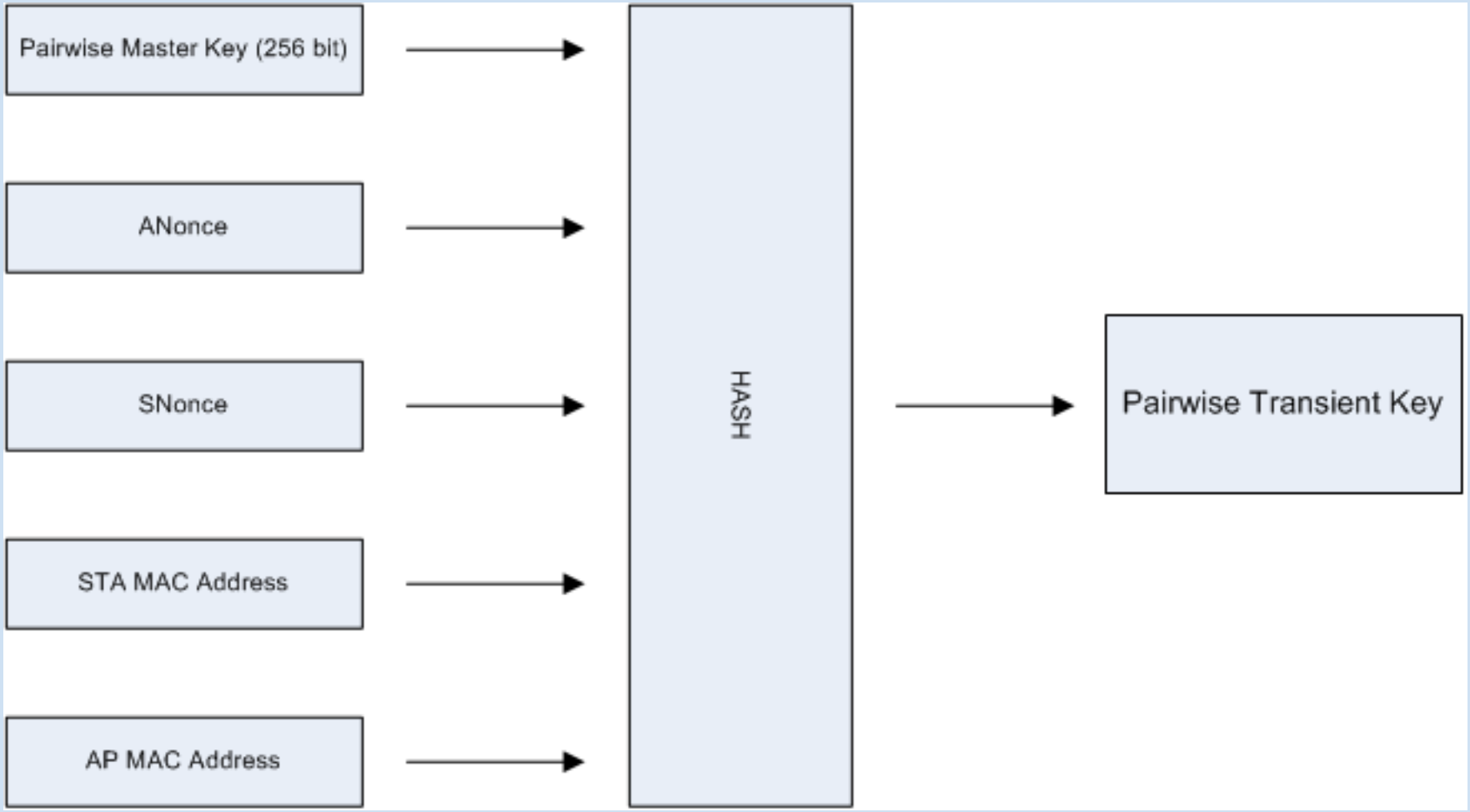
Network Interaction – WPA Authentication



Network Interaction – WPA – GTK



Network Interaction – WPA – PTK Construction



SEGURIDAD EN REDES WIRELESS

WPA (Wi-Fi Protected Access) - PSK

WPA-PSK (pre-shared key)

La comunicación es iniciada mediante el envío de un paquete tipo “EAPOL start” desde la estación al AP.
Seguidamente el AP genera un número aleatorio “ANonce” que es transmitido a la estación.

Ésta contesta remitiéndole otro número aleatorio llamado “SNonce“.

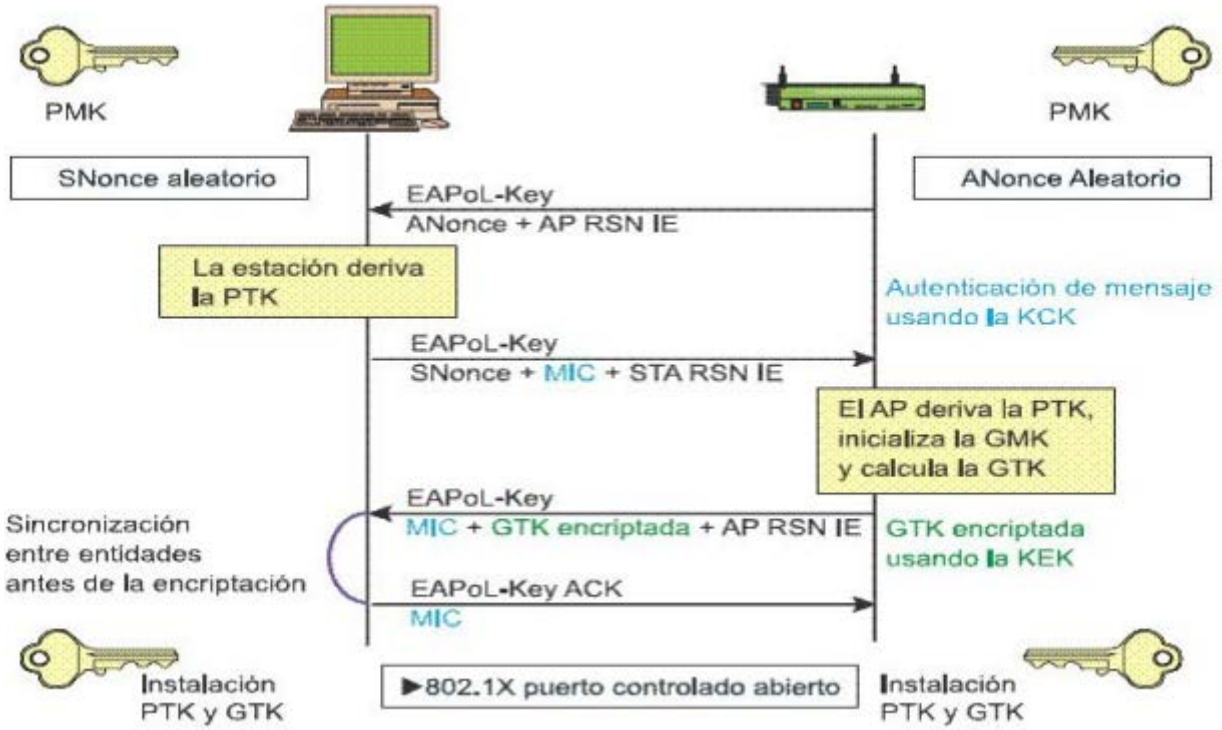
Llegado este punto_ambos pueden generar ya su PTK con la que cifrarán el tráfico unicast a partir de los valores mencionados.

A su vez, el AP esta en disposición de generar la GTK, procediendo a transmitirla a la estación de forma cifrada.
Como último paso, se envía un paquete de reconocimiento cerrando así el proceso de autenticación.

SEGURIDAD EN REDES WIRELESS

WPA (Wi-Fi Protected Access) - PSK

WPA-PSK (pre-shared key)



SOLUCIONES DE SEGURIDAD

Encriptación WPA2 (Wi-fi Protected Access)

WPA2 (IEEE 802.11i)

802.11i es el estándar del IEEE para proporcionar seguridad en redes WLAN.

Para la autentificación utiliza EAP.

Para la encriptaciónWPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard) ,mejor que TKIP, desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos.

Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol). CCMP es protocolo que utiliza AES (Advanced Encryption Standard) como algoritmo criptográfico y proporciona integridad y confidencialidad. Se basa en el modo CCM (Counter with CBC-MAC) del algoritmo de cifrado AES y utiliza llaves de 128 bits con IVs de 48 bits.

CCMP consta del algoritmo de privacidad que es el "Counter Mode" (CM) y del algoritmo de integridad y autenticidad que es el "Cipher Block Chaining Message Authentication Code" (CBC-MAC).

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS (Normal de funcionamiento) sino también para el modo IBSS (redes ad-hoc).

SOLUCIONES DE SEGURIDAD

Comparación WPA - - WPA2

TABLA COMPARATIVA :

	WPA	WPA2
Modo Enterprise	Autentificación: 802.1x / EAP	Autentificación: 802.1x / EAP
	Encriptación: TKIP/ MIC	Encriptación: AES-CCMP
Modo Personal	Autentificación: PSK	Autentificación: PSK
	Encriptación: TKIP/ MIC	Encriptación: AES-CCMP

Tanto en WPA como WPA2, en el modo Enterprise el sistema trabaja asignando a cada usuario una única clave de identificación, lo que proporciona un alto nivel de seguridad.

Para la autentificación ambos sistemas utilizan el 802.1x.

Para la encriptación WPA2 utiliza un algoritmo de cifrado mejor que el TKIP, el AES.

Para funcionamiento en la versión personal, se utiliza una clave compartida (PSK) que es manualmente introducida por el usuario tanto en el punto de acceso como en las máquinas cliente, utilizando para la encriptación o bien TKIP o AES. En este sentido las diferencias con WEP se basan en el algoritmo de cifrado de los datos.802.11i es el estándar del IEEE para proporcionar seguridad en redes WLAN.

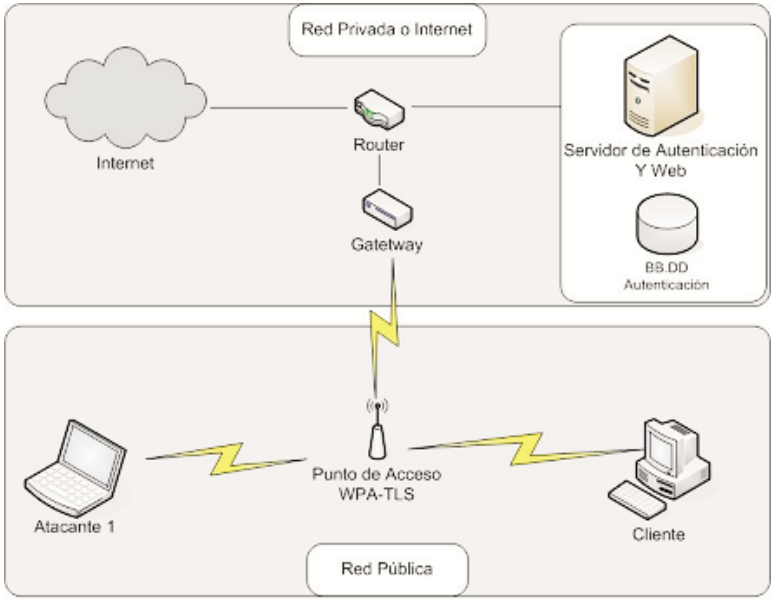
SEGURIDAD EN REDES WIRELESS

PORTALES CAUTIVOS

PRINCIPIO DE FUNCIONAMIENTO

Permite la validación de usuarios en nodos wireless. Usado para proporcionar conexión regulada a los usuarios de establecimientos públicos, hoteles, aeropuertos,
Se definen dos partes diferenciadas: la zona pública y la privada.

- En la zona pública están los nodos wireless que posibilitan la conexión de cualquier terminal;
- En la zona privada, normalmente Internet, se encuentra regulado por un sistema de autenticación que impide la navegación hasta que el usuario se valida.



SEGURIDAD EN REDES WIRELESS

PORTALES CAUTIVOS

VULNERABILIDAD

DNS tunneling

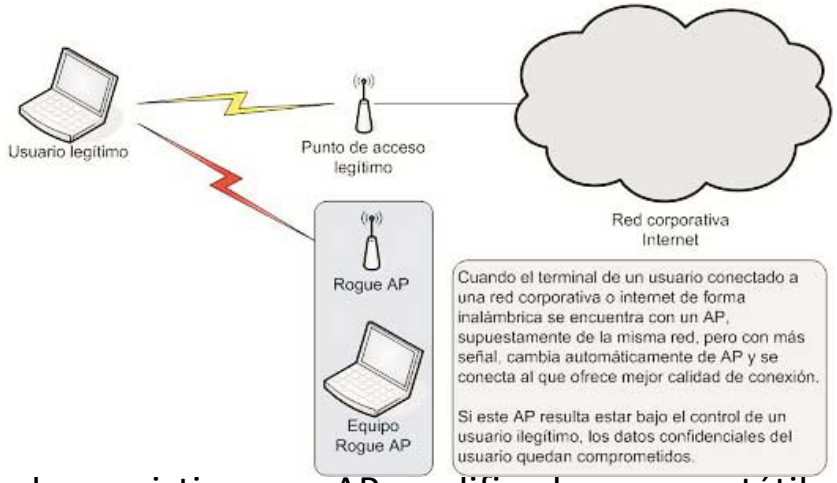
Debido a las características de la zona abierta de los sistemas que implantan este sistema de portales, se permite la asociación con el AP a cualquier cliente y el tráfico entre los clientes y el AP no va cifrado; por este motivo se puede capturar el tráfico de las conexiones con la zona privada.

SEGURIDAD EN REDES WIRELESS

ATAQUE ROGUE AP

PRINCIPIO DE FUNCIONAMIENTO

Consiste en colocar un punto de acceso bajo nuestro control cerca de las instalaciones de la víctima de forma que los clientes asociados o por asociar a esa red se conecten a nuestro AP en lugar de uno legítimo de la víctima debido a la mayor señal que recibe de nuestro AP.
Una vez conseguida la asociación al Rogue AP, el atacante puede provocar ataques de tipo DoS, robar datos de los clientes como usuarios y contraseñas de diversos sitios web o monitorizar las acciones del cliente.



El Rogue AP puede consistir en un AP modificado o un portátil con el software adecuado instalado y configurado. Este software ha de consistir en: Servidor http, Servidor DNS, Servidor DHCP y un Portal Cautivo con sus correspondientes reglas para redirigir el tráfico al portal.

SEGURIDAD EN REDES WIRELESS

ROGUE AP BÁSICO

PRINCIPIO DE FUNCIONAMIENTO

Todo este proceso de instalación y configuración se puede simplificar bastante mediante Airsnarf, herramienta que automatiza el proceso de configuración y arranque de un Rogue AP.
Se requiere que la tarjeta wireless sea compatible con HostAP, un driver específico que permite colocar la tarjeta en modo master, necesario para que nuestro terminal pueda comportarse como si fuese un AP.

El proceso de configuración que lleva a cabo Airsnarf consiste en simular el portal cautivo y arrancar el servidor http, configurar el servidor DHCP para que proporciones IP, gateway y DNS al cliente; evidentemente el gateway y el servidor DNS será el terminal del atacante convertido en Rogue AP.
Por último se configura el servidor DNS para que resuelva todas las peticiones con a la IP del atacante, de forma que se puedan redireccionar todas hacia el portal cautivo del Rogue AP.

Una vez el usuario introduce su usuario y contraseña en el portal cautivo, el atacante ya las tiene en su poder. Lo normal es cambiar la apariencia del portal cautivo para que sea igual a la del portal del sistema al que se está suplantando.

SEGURIDAD EN REDES WIRELESS

ROGUE AP BÁSICO

PRINCIPIO DE FUNCIONAMIENTO

Otra opción es dejar navegar al usuario normalmente pero redirigir determinadas páginas a otras copias locales con el fin de obtener usuarios y contraseñas.

Para ello se puede modificar el servidor DNS para resolver aquellas páginas que nos convengan a nuestra dirección local donde tendremos preparada una copia falsa de la página.

SEGURIDAD EN REDES WIRELESS

ROGUE RADIUS

PRINCIPIO DE FUNCIONAMIENTO

Es una ampliación del Rogue Básico, que incorporan un servidor RADIUS en el terminal del atacante. Para este fin se emplea comúnmente un servidor FreeRADIUS adecuadamente configurado para responder a las peticiones de los usuarios legítimos.

Este tipo de montaje se emplea contra sistemas que cuentan con servidores de autenticación mediante EAP de forma que el atacante pueda suplantar todos los dispositivos y servidores presentes en el sistema legítimo de forma convincente, autenticador y servidor de autenticación.

SEGURIDAD EN REDES WIRELESS

PRINCIPIO DE FUNCIONAMIENTO

Auditoria Wifi: realizar una Auditoria Wifi consiste en averiguar el grado de vulnerabilidad de la clave (de la encriptación) de nuestra red inalámbrica.

Para realizar auditorias disponemos de varios tipos de programas, algunos de ellos son los que proponemos en esta web pero día a día van surgiendo más recursos.