# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE ESTUDIOS SUPERIORES

## ACATLÁN

# SEGURIDAD
# EN
# REDES INALÁMBRICAS
# WI-FI (802.11)

**BAJO LA OPCIÓN DE TESINA**

**QUE PARA OBTENER EL TITULO DE:**

LICENCIADO EN
MATEMÁTICAS APLICADAS Y COMPUTACIÓN

PRESENTA:

**FRANCISCO ROJAS GARCÍA**

ASESORA: Lic. NASHELI LÓPEZ BAUTISTA

**ACATLÁN, EDO. DE MÉXICO** **FECHA: AGOSTO, 2006**

# Seguridad

# en

# Redes Inalámbricas

# Wi-Fi (802.11)

**Francisco Rojas García**

FES
UNAM
ACATLÁN

# Agradecimientos

A Dios por esta maravillosa experiencia de vida aquí en la Tierra, por permitirme ser y estar.

A mi abuelo, cuya alegría, convivencia, enseñanzas, sabiduría y recuerdos son inolvidables, y que durante toda mi infancia forjaron parte de mí y de los valores que ahora tengo.

A mi padre a quien siempre he admirado por su gran dedicación, esfuerzo, trabajo, entereza y valores. Sus enseñanzas, humildad y perspectivas me han brindado grandes frutos.

A mi madre por su amor, apoyo, comprensión y continua fuente de inspiración para terminar este trabajo.

A mis hermanos, por su tenacidad y convivencia familiar. Cada uno un ejemplo a seguir.

A mi esposa cuya entereza me sigue sorprendiendo. Por compartir y enseñarme otros valores y aspectos de la vida.

A mi hija, cuyo amor, ternura y sensibilidad me ha enseñado más de lo que yo le podía enseñar. Por esta maravillosa aventura de ser padre.

Y a esta, nuestra gran casa de estudios, que es la Universidad Nacional Autónoma de México que me permitió una formación humana, académica y cultural.

A mí, por darme la oportunidad de terminar un ciclo que había dejado abierto hace muchos años, por aprender a aprender, por un nuevo proyecto de vida y por reaprender muchas cosas que había aprendido mal.

A todos

Gracias!!!

Atentamente,

Francisco Rojas García

# SEGURIDAD EN REDES INALÁMBRICAS (WI-FI)

## ÍNDICE GENERAL

# INTRODUCCIÓN

## SEGURIDAD EN REDES INALÁMBRICAS Wi-Fi (802.11)

Este trabajo plantea la problemática que representan las redes inalámbricas en cuanto a seguridad y da a conocer los diferentes métodos que pueden implementarse para enfrentar y solucionar dicho problema. Se hace un análisis a la seguridad que se han planteado, tanto la IEEE como la Alianza Wi-Fi, para las redes inalámbricas mejor conocidas como 802.11 y Wi-Fi respectivamente. Se desglosan los estándares desarrollados, los problemas y fallas que han enfrentado así como las soluciones que han ofrecido hasta la fecha.

El primer Capítulo aborda los CONCEPTOS BÁSICOS DE LAS REDES INALÁMBRICAS. Da un repaso a sus fundamentos, antecedentes, tecnologías de transmisión, funcionamiento, los estándares sobre los cuales se basan y las organizaciones que los desarrollan, impulsan y aprueban hasta convertirlos en estándares internacionales.

El segundo Capítulo, HISTORIA DE LA SEGURIDAD EN REDES INALÁMBRICAS, está dedicado a la evolución de la seguridad en redes inalámbricas. Se explica en qué consiste la seguridad informática. Se expone cómo su medio de transmisión las hace enfrentar otros factores, retos, vulnerabilidades y tipos de ataques adicionales a los heredados por las redes cableadas.

El tercer Capítulo REDES INALÁMBRICAS SIN SEGURIDAD: SU SIMBOLOGÍA, DETECCIÓN Y PROBLEMÁTICA explica como se detectan las redes inalámbricas. Los diferentes métodos de localizar, usar y espiar estas redes que no han sido propiamente configuradas y por ende no están protegidas han propiciado un nuevo lenguaje y simbología que se han diseminado por todo el mundo y que ahora utilizamos diariamente para referirnos a estos fenómenos.

En el cuarto Capítulo BRINDANDO SEGURIDAD A LAS REDES INALÁMBRICAS se hace una propuesta de las opciones existentes para brindar seguridad a las redes inalámbricas, teniendo en cuenta dos panoramas:

1) Redes de uso doméstico o para pequeñas empresas con pocos recursos informáticos, financieros y de personal, pero que desean un buen nivel de seguridad.

2) Redes de uso empresarial con un alto requerimiento de seguridad y que cuentan con los recursos necesarios.

# CAPITULO I

# CONCEPTOS BÁSICOS DE LAS REDES INALÁMBRICAS (WLAN)

# I.1) HISTORIA DE LAS REDES INALÁMBRICAS (WLANS)

## I.1.A) LA RADIO. FUNDAMENTO DE LAS REDES INALÁMBRICAS (WLANS)

Las redes inalámbrica al igual que la radio se basan en las señales electromagnéticas. Después de una serie de estudios de las señales respecto de las frecuencias y su modulación, dieron por resultado la tecnología de la radiodifusión. Ésta es el fundamento de las redes inalámbricas.

El teórico escocés James Clerk Maxwell impulsó por primera vez la noción de las ondas electromagnéticas en 1864, al postular que éstas provienen de un cambio de dirección en la energía eléctrica.

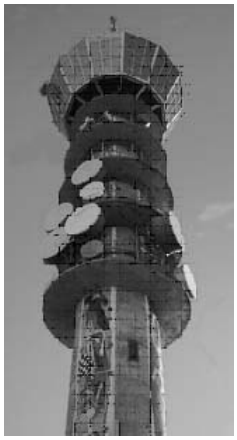


Figura I -1.Torre de Telecomunicaciones

Un dispositivo diseñado para producir ondas electromagnéticas mediante el cambio de la dirección de una corriente eléctrica, un proceso que se conoce como oscilación, es en esencia un transmisor. Un ejemplo de un transmisor y receptor de telecomunicaciones utilizado en nuestros días (Figura I-1).

Basándose en esto, el alemán Heinrich Hertz desarrolló un equipo en 1880 que envió y luego recibió ondas electromagnéticas a través del aire. Este equipo era capaz de incrementar el número de ondas que se producía en un período determinado, su frecuencia y su velocidad de cambio u oscilación. Su nombre se convirtió en una unidad común de medida para las frecuencias, donde 1 hertz (Hz) significa una oscilación o ciclo completo por segundo.

En el mundo de la radio la medida más común es el Kilo hertz (KHz) que representa miles de ondas de este tipo por segundo, mega hertz (MHz) son millones de ondas por segundo y así sucesivamente como se muestra en la Tabla I -1:

| UNIDADES DE FRECUENCIA | | |
|---|---|---|
| **Unidad de Frecuencia** | **Símbolo** | **Ciclos por segundo** |
| Hertz | Hz | 1 |
| Kilohertz | KHz | 1000 |
| Megahertz | MHz | 1 Millón |
| Gigahertz | GHz | 1 000 Millones |
| Terahertz | THz | 1 Billón |

TABLA I -1. CUADRO QUE MUESTRA LAS UNIDADES EN QUE SE MIDE LA FRECUENCIA

Las ondas de radio se propagan a través de diferentes medios físicos, como lo son el aire y el vacío. Al ser ondas electromagnéticas se propagan en estos dos medios a 300,000 Kilómetros por segundo aproximadamente, disminuyendo ligeramente en un medio como la atmósfera. En la Tabla I-2 se listan los factores que afectan las señales de radiofrecuencia y por ende a las comunicaciones de radio. En el Anexo A se explican aspectos de las frecuencias y su modulación.

| | |
|---|---|
| **ATENUACIÓN** | Es la pérdida de potencia sufrida por la señal al transitar por cualquier medio de transmisión. |
| **INTERFERENCIA** | Es cualquier proceso que altera, modifica o destruye una señal durante su trayecto en el canal existente entre el emisor y el receptor. |
| **DISTORSIÓN** | Deformación de una señal en cuanto a su amplitud, frecuencia ó fase. |
| **REFLEJOS** | Cambio de dirección de las ondas electromagnéticas que inciden sobre una superficie o cuerpo.. |
| **ASINCRONÍA** | Cuando la señal pierde su sincronía o es susceptible de desarrollarse con independencia del desarrollo de otros procesos. |

TABLA I-2. FACTORES QUE AFECTAN A LAS ONDAS ELECTROMAGNÉTICAS.

## I.1.B) ANTECEDENTES DE LAS REDES INALÁMBRICAS

Los inicios de las redes inalámbricas de área local (WLAN) se remontan a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza. Consistía en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 del IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones continuaron con infrarrojos y con microondas, utilizando el esquema del espectro extendido ("spread spectrum"), siempre a nivel de laboratorio.

En mayo de 1985 tras cuatro años de estudios, la FCC[1], asignó las bandas de frecuencias: 902 a 928 MHz, 2.400 a 2.4835 GHz, 5.725 a 5.850 GHz a las redes inalámbricas basadas en espectro extendido. Estas frecuencias son un subconjunto de las asignadas exclusivamente para fines industriales, científicos y médicos: ISM (Industrial, Scientific and Medical). ISM es para uso comercial sin licencia, es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide quién debe trasmitir en esa banda.
La asignación de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezara a dejar ya el laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 MBPS, el mínimo establecido por el IEEE 802 para que una red sea considerada como tal.

En 1992 se crea Winforum, un consorcio dirigido por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los Sistemas de Comunicación Personal (PCS - Personal Communications Systems). Ese mismo año, el Instituto de Estándares y Telecomunicaciones Europeo (ETSI - European Telecommunications Standards Institute), a través del comité ETSI-RES 10, inicia la creación de una norma denominada HiperLAN - Red de Alto Rendimiento (High Performance LAN) y en 1993 les asigna las bandas de 5.2 y 17.1 GHz. En ese mismo año se constituye la Asociación para Datos Infrarrojos (IRDA - Infrared Data Association) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos.

[1] FCC - (Federal Communications Commission). Agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones.

En 1996, un grupo de empresas del sector de informática móvil y de servicios forman el Foro de Interoperabilidad para WLANs (WLI Forum - Wireless LAN Interoperability Forum) se unen para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios ínteroperativos. Entre los miembros fundadores de WLI Forum se encuentran empresas como ALPS Electronics, AMP, Data General, Contron, Seiko, Epson y Zenith Data Systems.

Finalmente en 1997 la IEEE aprueba el primer estándar de redes inalámbricas, el 802.11, especificando una interfaz aérea entre un cliente inalámbrico y una estación base o entre dos clientes inalámbricos.

## I.1.C) ORGANISMOS INTERNACIONALES DE NORMALIZACIÓN

Existen instituciones que se encargan de establecer los estándares o normas a escala mundial para tener una base común de referencia a partir de la cual se pueda trabajar ordenadamente tanto en el desarrollo tecnológico como en otras áreas del conocimiento.

Ante el desarrollo de dispositivos de diferentes fabricantes, se hizo necesaria la existencia de recomendaciones (contenidas en los estándares), para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidad.

La normalización o estandarización es la redacción y aprobación de normas. Las normas son documentos técnicos con las siguientes características:

a) Contienen especificaciones técnicas de aplicación voluntaria.
b) Son elaborados por consenso de las partes interesadas:
    i. Fabricantes
    ii. Administraciones
    iii. Usuarios y consumidores
    iv. Centros de investigación y laboratorios
    v. Asociaciones y Colegios Profesionales
c) Están basados en los resultados de la experiencia y el desarrollo tecnológico.
d) Son aprobados por un organismo nacional, regional o internacional de normalización.
e) Están disponibles al público.

Las normas ofrecen un lenguaje común de comunicación entre los distintos agentes que participan en las transacciones comerciales, jurídicas, tecnológicas y son un modelo necesario de confianza entre sus participantes.

Algunos de los organismos internacionales que crean, definen y proponen estándares internacionales oficiales abiertos a la industria a través de un proceso abierto a las compañías son:

IEEE - *Institute of Electrical and Electronics Engineers*
IETF - *Internet Engineering Task Force*
ISO - *International Standards Organization*
ITU - *International Telecommunications Union*
ETSI - *European Telecommunications Standards Institute*

### IEEE

El Instituto de Ingenieros Eléctricos y Electrónicos se creó en los E. U. en 1963 a partir de otras instituciones como el AIEE (American Institute of Electrical Engineers) y el IRE (Institute of Radio Engineers). Es una asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros de telecomunicaciones, ingenieros electrónicos e Ingenieros en informática. Su trabajo es promover la creatividad, el desarrollo y la integración para compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales.
Del comité de Normalización de Redes Locales (IEEE 802) se pueden destacar las normas siguientes: 802.3 - Ethernet (CSMA/CD), 802.4 - Token Bus, 802.5 - Token Ring, 802.11 - Redes Inalámbricas (CSMA/CA).

### IETF

El Grupo de Trabajo de Ingeniera para Internet (IETF - Internet Engineering Task Force) tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Fue creada en los E. U. en 1986.

### ISO

La Organización Internacional para la Estandarización es una organización internacional no gubernamental, compuesta por representantes de los cuerpos de estandarización nacionales, que produce estándares mundiales industriales y comerciales.
ISO coopera estrechamente con la Comisión Electrotécnica Internacional (IEC - International Electrotechnical Comisión), que es responsable de la estandarización de equipos eléctricos.
Es un error común el pensar que ISO significa International Standards Organization (Organización Internacional de Estándares), o algo similar; ISO no es un acrónimo; proviene del griego iso, que significa igual. En inglés su nombre es International Organization for Standarization, mientras que en francés se denomina Organisation Internationale de Normalisation; el uso del acrónimo conduciría a nombres distintos: IOS en inglés y OIN en francés, por lo que los fundadores de la organización eligieron ISO como la forma corta y universal de su nombre.

### ITU

La Unión de Telecomunicaciones Internacional (ITU - International Telecommunication Union) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas Administraciones y Empresas Operadoras.

## I.1.D) ASOCIACIONES DE LA INDUSTRIA

Éstas se crearon para promover el crecimiento de la industria a través de la educación y promoción, brindando información objetiva sobre la industria en general, tecnologías, tendencias y oportunidades independientemente de la tecnología. La organización más importante en esta categoría es la WLANA (Wireless Local Area Network Association), cuya misión es ayudar y fomentar el crecimiento de la industria a través de la educación que puede caracterizarse por asociaciones industriales y comerciales.

Instituciones como éstas promueven la competencia y avances tecnológicos, lo que significa mejores soluciones para los usuarios de redes inalámbricas e incrementar el crecimiento de la industria. La fuerza del mercado decide el valor de cada organización.

## I.1.E) ALIANZAS DE TECNOLOGÍA

Típicamente, una alianza de tecnología se forma para introducir al mercado una tecnología o protocolo específico y proveer interoperabilidad y certificación de productos de diferentes compañías que utilizan esa tecnología o protocolo. Ejemplos de este tipo de organizaciones son las siguientes:

**BLUETOOTH SIG**
Basado en Bluetooth, que utiliza tecnología de radiofrecuencia para proveer conectividad a Internet (a bajo costo) a computadoras portátiles, teléfonos móviles u otros dispositivos móviles formando redes conocidas como Redes de área Personal (PAN - Personal Area Networks).

**HIPERLAN1, HIPERLAN ALLIANCE E HIPERLAN2 GLOBAL FORUM**
Organizaciones europeas que utilizan enlaces de radio de alto desempeño a frecuencias en el rango de los 5 GHz.

**HOMERF**
Basada en una especificación para comunicaciones inalámbricas en hogares conocida por sus siglas en inglés SWAP (Shared Wireless Access Protocol). El HRFWG (Grupo de Trabajo para radiofrecuencia casera - HomeRF Working Group) se fundó para proveer los cimientos a un amplio rango de dispositivos al establecer una especificación abierta a la industria para comunicaciones digitales inalámbricas, entre PCs y dispositivos domésticos alrededor de los hogares.

**WLI Forum**
WLIF (Wireless LAN Interoperability Forum), Antigua organización que estableció un estándar ínter-operable en 1996 conocido como OpenAir y posteriormente promovió el 802.11. OpenAir es una tecnología de espectro extendido con salto de frecuencia a 2.4 GHz. Esta organización desapareció en el 2001.

**ALIANZA WI-FI**
"The Wi-Fi Alliance" se formó en agosto de 1999 por las compañías 3Com, airones wireless Communications, Harris Semiconductor, Lucent Technologies, Nokia y Symbol Technologies. Certifica la interoperabilidad de productos WLAN basados en la especificación y promover el término Wi-Fi como el nombre de marca global para los productos basados en 802.11.Solo a aquellos productos que han pasado las pruebas de la Alianza Wi-Fi se les permite referirse como Wi-Fi Certificados. A éstos se les requiere llevar un sello de identificación en sus empaques que indique tanto su estatus de Certificación, así como la banda de radio frecuencia en la que opera (2.5 GHz para 802.11b/g y 5GHz para 802.11a).

Este grupo fue originalmente conocido como **WECA** (Wireless Ethernet Compatibility Alliance) pero cambio su nombre en Octubre de 2002 para reflejar mejor la marca Wi-Fi que quería construir.

En la Tabla I -3 se proporciona un listado de los organismos de estándares, asociaciones y alianzas relacionados con redes inalámbricas.

| NOMBRE DE LA ORGANIZACIÓN | MISIÓN | TECNOLOGÍA PROMOVIDA |
|---|---|---|
| **Asociaciones de la Industria** | | |
| Wireless LAN Asociación (WLANA). http://www.wlana.org | Promueve el uso de tecnología de red inalámbrica y trabaja para elevar la conciencia del consumidor respecto del uso y disponibilidad de las WLANs. | LANs, WLANs, LAN a LAN y Redes de Área Personal. |
| **Alianzas de Tecnología** | | |
| WECA ó Alianza Wi-Fi http://www.wi-fi.org | Certifica la interoperabilidad de productos Wi-Fi (IEEE 802.11) y promueve Wi-Fi como el estándar global del mercado. | Wi-Fi: IEEE 802.11 |
| Bluetooth http://www.bluetooth.com/ | Conduce el desarrollo de las especificaciones Bluetooth. | Bluetooth: IEEE 802.15 |
| Foro OFDM http://www.ofdm-forum.org | Promueve un estándar compatible con OFDM. | OFDM |
| HomeRF http://www.homerf.org | Desarrolla especificaciones para comunicaciones inalámbricas en el hogar. | Protocolo HomeRF |
| Alianza HIPERLAN http://www.hiperlan.com | Acelera el despliegue mundial de sistemas HiperLAN/1. | HiperLAN/1 |
| Foro Global HiperLAN2 http://www.hiperlan2.com | Maneja la adopción de HiperLAN2 como la tecnología global de comunicación en la banda de los 5 GHz. | HiperLAN/2 |
| **Organismos de Estándares** | | |
| IEEE - Instituto para Ingenieros Eléctricos y Electrónicos. (Institute for Electrical and Electronics Engineers) http://www.ieee.org | Desarrolla estándares relevantes del mercado. | 802.11 y 802.15 |
| ETSI - Instituto de Estándares y Telecomunicaciones Europeo (European Telecommunications Standards Institute) http://www.etsi.org | Produce estándares de telecomunicaciones usados en Europa. | HiperLAN/1 HiperLAN/2 |
| **Agencias Reglamentadoras** | | |
| FCC - Comisión Federal de Comunicaciones. (Federal Communications Commission) http://www.fcc.gov | La FCC es una agencia del Gobierno de los Estados Unidos que hace leyes, define las bandas de frecuencia, niveles de potencia de transmisión, modulación de tecnologías y otras formas en las que los dispositivos WLAN deben operar. | Varios |
| **Laboratorios de Pruebas** | | |
| Universidad de New Hampshire http://www.iol.unh.edu | Pruebas de Interoperabilidad. | Varios |

TABLA I-3. ORGANISMOS DE ESTÁNDARES, ALIANZAS Y ASOCIACIONES PARA REDES INALÁMBRICAS

# I.2) TECNOLOGÍAS DE TRANSMISIÓN PARA LAS WLANS

El IEEE 802.11 define tres variantes de transmisión de la capa física (del modelo OSI): el Infrarrojo y dos de radiofrecuencia que requieren modulación de espectro extendido: DSSS y FHSSS. Solo éstas últimas tienen presencia significativa en el mercado.

Existen dos tipos de propagación de señales: Banda angosta y de Banda extendida.

## I.2.A) BANDA ESTRECHA O ANGOSTA

Un sistema de radio de banda angosta transmite y recibe información en una frecuencia específica. La banda angosta mantiene la frecuencia de la señal de radio tan angostamente posible (Figura I-2) para conducir la información. El cruzamiento no deseado entre canales se evita al coordinar cuidadosamente distintos usuarios en diferente canal de frecuencia.

Por ejemplo, en un sistema de radio, la privacidad y la no-interferencia se incrementan por el uso de frecuencias separadas. El radio receptor filtra aquellas frecuencias que no son de su competencia. La desventaja de esta tecnología es el uso de una frecuencia para cada usuario, lo que es inútil si se tienen muchos usuarios.

## I.2.B) ESPECTRO EXTENDIDO

Para operar legalmente en el espectro ISM de 2.4 GHz en Estados Unidos y muchos otros países, se debe usar un tipo de propagación de señales.

Los productos 802.11 usan técnicas de espectro extendido (también llamado espectro ensanchado, espectro esparcido, espectro disperso, o Spread Spectrum) para transmitir sus señales, la cual es una tecnología de banda amplia (Figura I-2) desarrollada por los militares estadounidenses que provee comunicaciones seguras, confiables y de misión crítica. La tecnología de espectro extendido está diseñada para intercambiar eficiencia en ancho de banda por confiabilidad, integridad y seguridad.

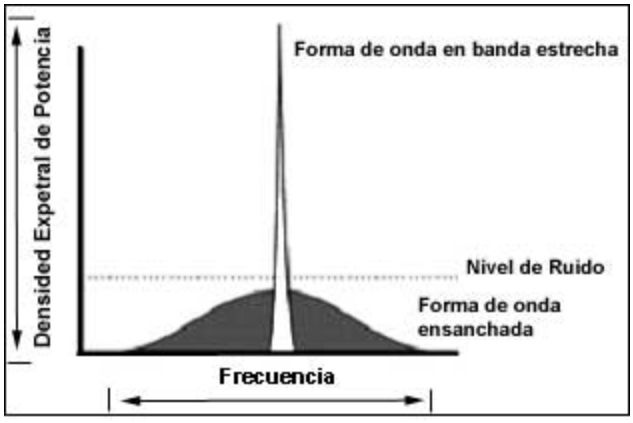



FIGURA I-2. ESPECTRO EXTENDIDO Y ANGOSTO

Una analogía utilizada para entender el concepto de la propagación de señales de espectro extendido es la de una serie de trenes que parten de una estación. La carga se coloca en cada tren, los cuales, parten al mismo tiempo. Las duplicaciones de la carga son comunes en el espectro extendido de modo que cuando lleguen datos corrompidos de manera excesiva, o no logren llegar al destino, las redundancias inherentes a esta arquitectura permiten recuperar la información.

Existen dos tipos de espectro extendido disponibles para 802.11:

a) Salto de Frecuencia (Frequency Hopping Spread Spectrum: FHSS)
b) Secuencia Directa (Direct Sequence Spread Spectrum: DSSS)

DSSS se desempeña mejor, pero FHSS es más resistente a la interferencia. Aunque OFDM (Ver Anexo B) es una técnica para propagar las señales a través de un ancho de banda determinado, no es, por definición una técnica de espectro extendido. 802.11a y 802.11 g usan OFDM como su técnica de propagación.

La señal de espectro extendido, puede coexistir con señales en banda estrecha, ya que sólo les aportan un pequeño incremento en el ruido. En lo que se refiere al receptor de espectro extendido, él no ve las señales de banda estrecha, ya que está escuchando un ancho de banda mucho más amplio gracias a una secuencia de código preestablecido.

La interferencia tiende a cubrir más de un canal a la vez. Por tanto, los sistemas DSSS tienden a perder más datos debido a la interferencia, ya que la información se envía a través de canales secuenciales. Los sistemas FHSS "saltan" entre los canales con un orden no secuencial. El mejor de los sistemas FHSS ajusta la selección de los canales, de manera que los canales con interferencia alta se evitan cuando se mide en ellos tasas de bits excesivamente bajas.

## I.2.B. I) ESPECTRO EXTENDIDO CON SALTO DE FRECUENCIA (FHSS)

Con la arquitectura FHSS, los trenes salen en un orden diferente; es decir, no en secuencia desde el Tren 1 hasta el Tren N. En el mejor de los sistemas FHSS los trenes que experimentan una interferencia no se envían de nuevo, por esas vías, hasta que la interferencia desaparece.

El FHSS (Frequency Hopping Spread Spectrum) aparece antes de la 2ª guerra mundial y utiliza una portadora de banda angosta que cambia de frecuencia, cada 400 milisegundos, en una secuencia establecida previamente a la transmisión. En la (Figura I-3) la secuencia sería 2,3,1,4,6,5. El transmisor y el receptor deben estar sincronizados, comunicándose por un canal de control que cambia de frecuencia en cada momento. El FHSS es utilizado para comunicaciones en distancias cortas, en aplicaciones donde por lo general se tiene una cantidad de receptores en un área cercana al punto de acceso. Utiliza 75 subcanales de 1 Mhz cada uno.

Esta tecnología esta siendo desechada y solo un proveedor de chips la sigue soportando.

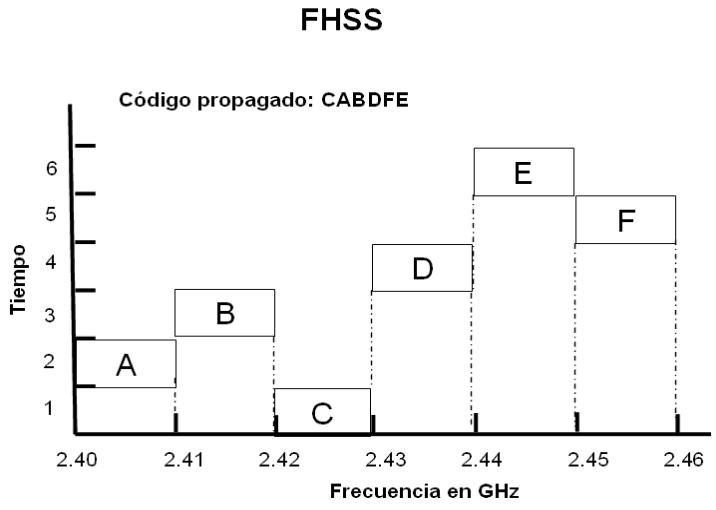



FIGURA. I-3. ESPECTRO EXTENDIDO MEDIANTE SALTOS DE FRECUENCIA.

## I.2.B. II) ESPECTRO EXTENDIDO EN SECUENCIA DIRECTA (DSSS)

Mediante DSSS, todos los trenes parten en el mismo orden que comienza con el Tren 1 y termina con el Tren N, dependiendo de la cantidad de canales que asigne el sistema de espectro extendido

El DSSS (Direct Sequence Spread Spectrum) genera un patrón de bits redundante (Figura I-4) llamado código chip de 11 elementos. Cada bit a ser transmitido es convertido a código chip. Es por esto que si uno o más bits se dañan, técnicas estadísticas embebidas dentro del radiotransmisor podrán recuperar la señal original sin necesidad de retransmisión.

Esta técnica divide la banda ISM 2.4Ghz en 14 canales de 22 Mhz cada uno. El desempeño de DSSS puede mejorar al incrementar la velocidad del reloj o la complejidad de la modulación.

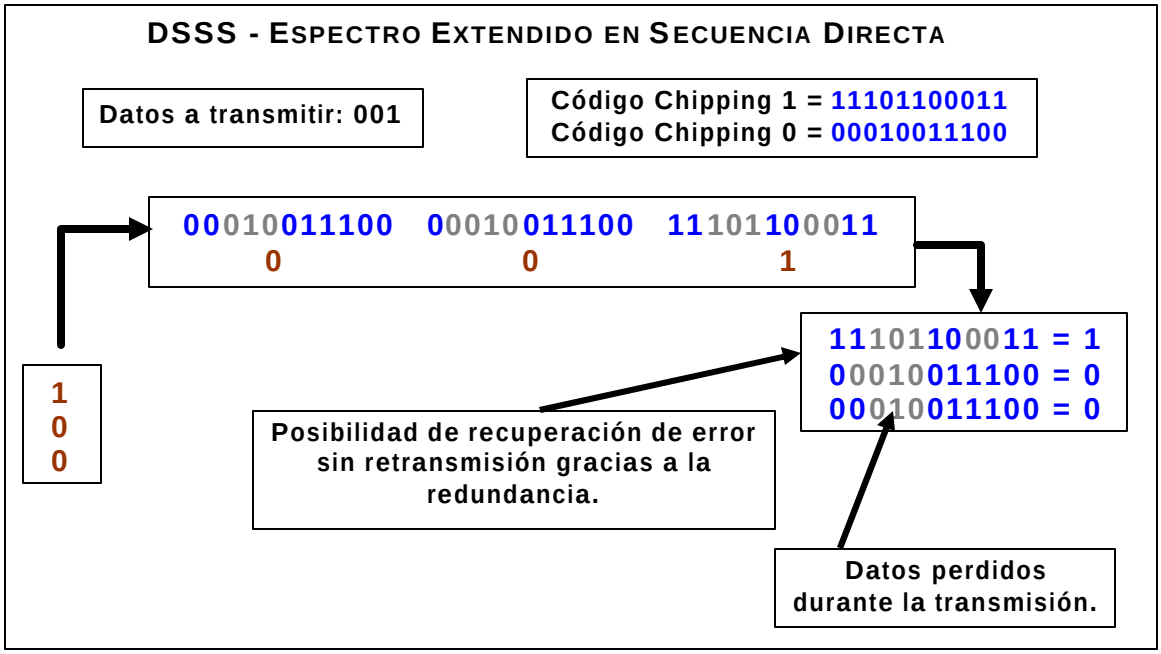



FIGURA. I-4. CÓDIGO CHIP DE 11 ELEMENTOS POR CADA BIT A TRANSMITIR.

## I.2.C) VENTAJAS Y DESVENTAJAS DEL ESPECTRO EXTENDIDO

El espectro extendido tiene muchas propiedades únicas y diferentes que no se pueden encontrar en ninguna otra técnica de modulación. Para verlo mejor, se listan debajo algunas ventajas y desventajas que existen en los sistemas típicos de espectro extendido:

**VENTAJAS**

- Resiste todo tipo de interferencias, tanto las no intencionadas como las malintencionadas (más conocidas con el nombre de jamming), siendo más efectivo que las de banda estrecha.
- Tiene la habilidad de eliminar o aliviar el efecto de las interferencias multitrayecto.
- Se puede compartir la misma banda de frecuencia con otros usuarios.
- Confidencialidad de la información transmitida gracias a los saltos seudo aleatorios.
- FHSS es mejor contra las interferencias.
- DSSS es superior en la recuperación de errores.

**DESVENTAJAS**

- Utilización de más ancho de banda. DSSS la utiliza más eficientemente que FHSS.
- La implementación de los circuitos es en algunos casos muy compleja.
- Incompatibilidad: FHSS y DSSS no pueden coexistir.
- Velocidad de 2 Mbps máxima en FHSS debido a su limitación de frecuencia a 1 GHz.

## I.2.D) TRANSMISIONES QUE NO SON PARTE DEL ESPECTRO EXTENDIDO

Es pertinente mencionar que existen equipos que utilizan la mismas frecuencias que las redes inalámbricas, pero no transmiten información. Sus aplicaciones estan orientadas al área Industrial, Científica y Médica, lo que se denomina como ISM (Industrial Scientific and Medical).
En caso de tener una red inalámbrica en la misma área donde existan alguno de estos equipos, se tendrá una gran interferencia en la red. Ejemplos de estos equipos son: limpiadores domésticos de joyería, humidificadores ultrasónicos, calefacción industrial, hornos de microondas, etcétera.

# I.3) COMO FUNCIONAN LAS WLANS

## I.3.A) ELEMENTOS DE UNA RED INALÁMBRICA

**Adaptador de red**: es una tarjeta de red inalámbrica, conocida como NIC por sus siglas en inglés (Network Interface Card - Tarjeta de Interfase a la Red). Permite a un equipo (cliente, STA ó host) conectarse con otros equipos inalámbricos o con un punto de acceso.

**Punto de Acceso**: Son el centro de las comunicaciones a través del cual una red inalámbrica se conforma. También permite establecer comunicación con una red cableada, actuando como un puente (Bridge) entre ambas y puede extender la cobertura de la red inalámbrica haciendo conexiones punto a punto entre puntos de acceso.

**Protocolo de Comunicación**. El protocolo soportado por defecto es el TCP/IP (Ver Anexo D), aunque puede utilizar cualquier otro. Soporta los sistemas operativos de red habituales, lo que es una gran ventaja para los usuarios que pueden seguir utilizando sus aplicaciones habituales, con independencia del medio empleado, sea por cable o por radio.

**Identificador SSID (Service Set Identifier).** Este nombre o identificador es definido durante la configuración del equipo inalámbrico. Permite definir a que red se pertenece.

## I.3.B) 802.11 NO ES ETHERNET

Es importante aclarar esto ya que las redes inalámbricas se diferencian de las redes cableadas en las dos primeras capas (Figuras I-5 y I-6) del modelo OSI: Física y Enlace de Datos (Véase Anexo C).

La capa física, se encarga de las señales de radiodifusión a transmitir a nivel de bits(Figura I-7).
La segunda capa, enlace de datos, se divide en dos subcapas y tiene funciones de control de flujo e integridad de las comunicaciones:

LLC - Control Lógico de Enlace (Logical Link Control) ó 802.2
MAC - Control de Acceso al Medio (Media Access Layer)

La subcapa LLC, también conocida como 802.2 intercomunica a las capas 1 y 3 (Figura I - 7).

La subcapa MAC, tiene una dirección de 20 bytes en base hexadecimal, es única a nivel mundial y es establecida por el fabricante para identificar cada dispositivo en una red. Es por esto que esta capa es también conocida como *capa de direccionamiento MAC*.


FIGURA I - 5. CAPAS DEL MODELO OSI

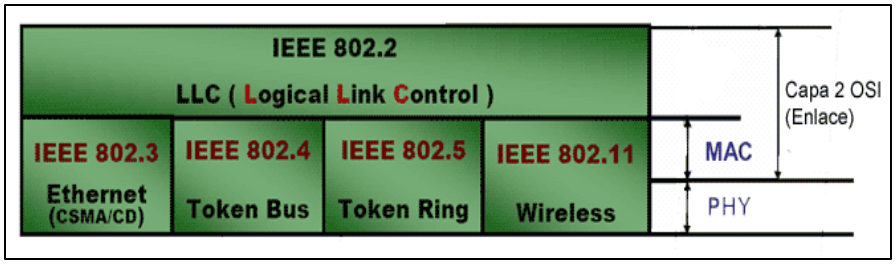



FIGURA I - 6. VISUALIZACIÓN DE LA DIVISIÓN DE LAS CAPAS 1 Y 2.

Ambas capas se encuentran implementadas en los dispositivos de red, los cuales tienen procesadores dedicados exclusivamente a éstas tareas.

Adicionalmente, una red Ethernet convencional utiliza un protocolo de acceso al medio denominado CSMA/CD - Acceso múltiple con sensor de portadora / Detección de colisiones (Carrier Sense Multiple access /Collision Detection).

El estándar de las redes inalámbricas, el 802.11, usa un protocolo diferente, que se conoce como CSMA/CA - Accesos múltiples con sensor de portadora / Evasión de colisiones (Carrier Sense Multiple Access / Collision Avoidance), para asegurar que la cantidad de colisiones se mantenga a un nivel mínimo dentro del dominio. De hecho, en un ambiente inalámbrico, la señal transmitida es tan potente localmente que la detección de colisiones no es una opción.

Es por esto que los puntos de acceso actúan como puentes entre una red inalámbrica y una red cableada, intercambiando paquetes entre una red y otra; como si fueran traductores entre un idioma y otro. Su funcionamiento es transparente para el usuario por lo cual son denominados puentes transparentes.

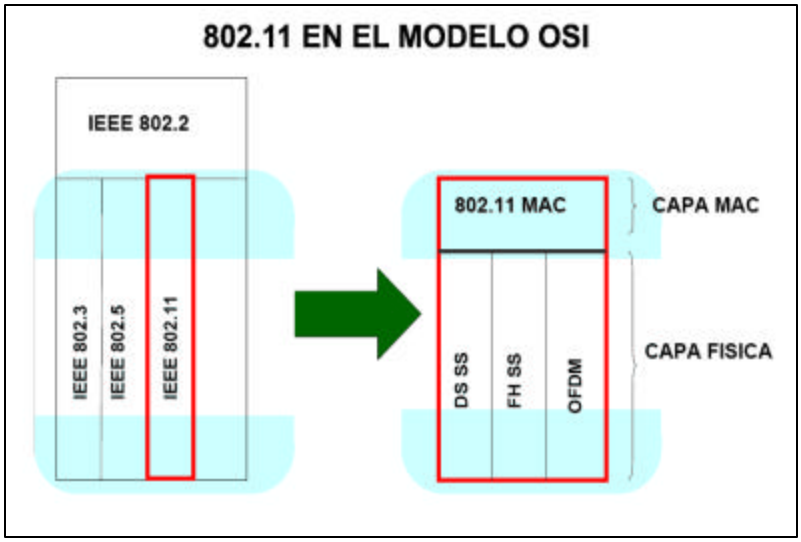



FIGURA I-7. MÉTODOS DE SEÑALIZACIÓN EN 802.11 BAJO EL MODELO OSI

## I.3.C) FUNCIONAMIENTO DE UNA WLAN

Las redes de área local inalámbricas (WLAN) se pueden definir como aquellas que utilizan señales electromagnéticas ó tecnología de radiofrecuencia (Figura I-8) para comunicar y compartir recursos entre sus dispositivos en lugar de los cables (coaxial, UTP ó fibra óptica) que se utilizan en las redes convencionales.

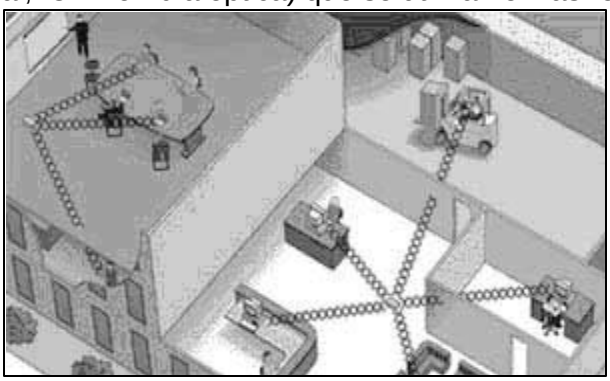


FIGURA. I-8. RED LOCAL INALÁMBRICA

En una configuración típica de WLAN, un dispositivo transmisor / receptor, llamado **Punto de Acceso** (Figura I-9), puede soportar un grupo pequeño de usuarios y puede funcionar dentro de un rango de hasta 100 metros, denominándose dominio a esta área de cobertura (Figura I-10).

Los clientes, para asociarse o pertenecer a una red inalámbrica se configuran con el mismo identificador (SSID) del punto de acceso, llamándose a esto asociación abierta. La asociación encriptada consiste en activar un mecanismo de seguridad en las transmisiones como lo es WEP o WAP, los cuales veremos en el capítulo 2.

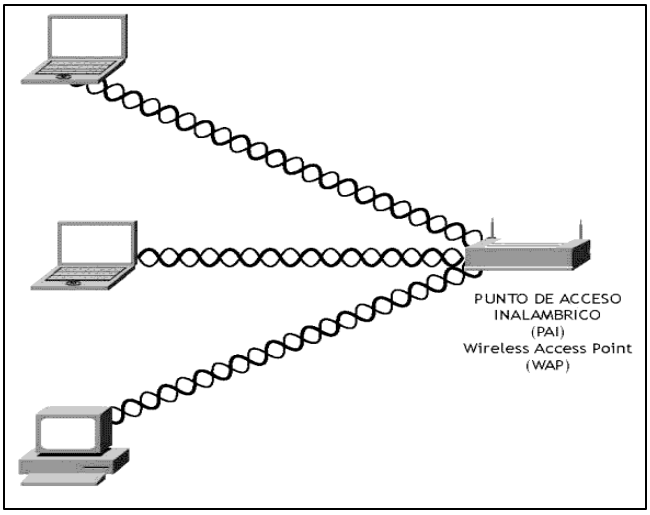



FIGURA. I-9. PUNTO DE ACCESO INALÁMBRICO

Una vez asociados, los clientes reciben una dirección IP, la cual es ligada a su dirección MAC, con la cual podrán trabajar en sus aplicaciones.

El Punto de Acceso puede ser montado esencialmente donde sea de tal modo que se obtenga la cobertura de radio deseada.

Otra función de un punto de acceso es la de conectar una WLAN a la red cableada, actuando como un puente entre ambas redes.

Los clientes acceden a la WLAN usando adaptadores ó tarjetas de red inalámbricas por ejemplo: tarjetas PCMCIA, USB, PCI ó dispositivos completamente integrados a las agendas o computadoras de mano (handheld).

Las conexiones inalámbricas son transparentes al Sistema Operativo de Red (NOS - Network Operating System) o al sistema operativo de la máquina en la que se este trabajando.

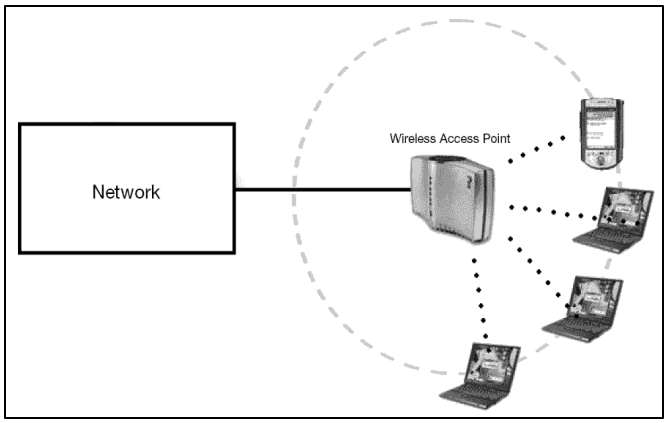



FIGURA I-10. PUNTO DE ACCESO Y SU COBERTURA O DOMINIO.

## I.3.D) MODOS DE OPERACIÓN: INFRAESTRUCTURA Y PUNTO A PUNTO

### INFRAESTRUCTURA - BSS

Esta configuración se logra al instalar un Punto de Acceso cuya cobertura es llamada célula, cada una de éstas contribuye a formar lo que se denomina arquitectura celular (Figura I-11) también conocida como BSS[2]. Cada punto de acceso actúa como regulador de tráfico entre los diferentes equipos móviles. Tiene por lo general una cobertura de 100 metros a la redonda, dependiendo del número y tipo de obstáculos que haya en la zona.

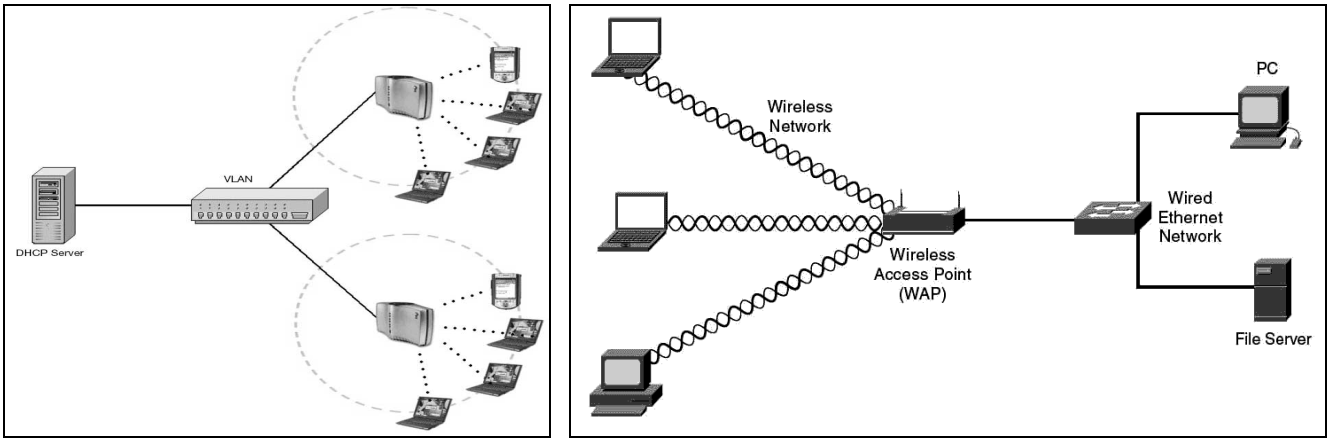



FIGURA I-11. REDES INALÁMBRICAS OPERANDO EN MODO DE INFRAESTRUCTURA.

Un Punto de Acceso también permite la conectividad a la red cableada, con lo cual, las estaciones inalámbricas pueden ser agregadas rápida y fácilmente a la red corporativa; permitiendo hacer uso de los recursos bajo la misma infraestructura, de ahí su nombre.

### PUNTO A PUNTO - (AD-HOC, IBSS)

En esta configuración, denominada IBSS[3], Ad Hoc ó P2P[4], los equipos móviles se conectan unos con otros, sin necesidad de que exista un punto de acceso, utilizando su **tarjeta de red inalámbrica** para llevar a cabo dicha conexión, como se muestra en la (Figura I-12).

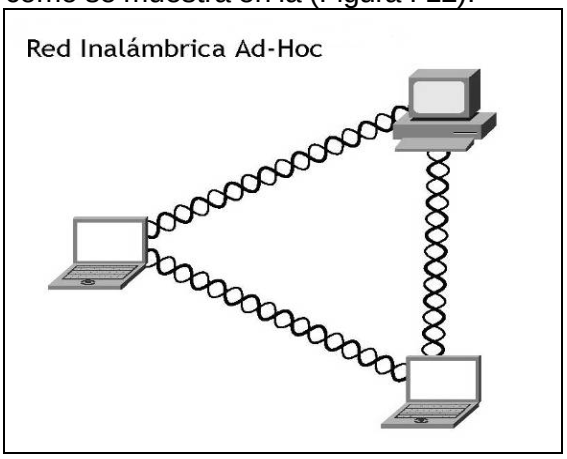



FIGURA. I-12. RED INALÁMBRICA IBSS, AD HOC O PUNTO A PUNTO (P2P).

[2] BSS - Basic Service Set - Conjunto de Servicios Básicos
[3] IBSS - Independet Basic Service Set - Conjunto de Servicios Básicos Independientes.
[4] P2P - Point to Point - Punto a Punto.

## I.3.E) PRODUCTIVIDAD CON LAS WLANS

En los últimos años, las redes locales inalámbricas (WLAN) han ganado muchos adeptos y popularidad en áreas tales como hospitales, fábricas, mercados, bodegas, bibliotecas, tiendas de autoservicio y departamentales, Universidades, Grandes Almacenes, aeropuertos, restaurantes, pequeños negocios, corporaciones, etc. Las redes inalámbricas permiten a los usuarios acceder a la información y los recursos en tiempo real sin necesidad de estar físicamente en un solo lugar gracias a su flexibilidad y rapidez de instalación, movilidad, costo - beneficio, escalabilidad y la simplicidad de las WLANs abren un sinfín de aplicaciones que no son posibles con las redes cableadas.

Con las WLANs la red por sí misma es móvil y establece nuevas aplicaciones añadiendo flexibilidad a la red y lo más importante, incrementa la productividad y eficiencia en las actividades diarias de la empresa. Un usuario de una red inalámbrica puede transmitir y recibir voz, datos, y video dentro o entre edificios o Campus universitarios.

Muchos de los fabricantes de computadoras y equipos de comunicaciones como PDAs (Personal Digital Assistants; Asistentes personales digitales), módems, microprocesadores inalámbricos, lectores de punto de venta y otros dispositivos, están introduciendo aplicaciones en soporte a las actividades inalámbricas. Las nuevas posibilidades que ofrecen las WLANs son permitir una fácil incorporación de nuevos usuarios a la red, proporcionando una alternativa de bajo costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red corporativa.

# I.4) ESTÁNDARES ACTUALES

## I.4.A) WI-FI - FIDELIDAD INALÁMBRICA

Generalmente se piensa que el término Wi-Fi (Wireless Fidelity) es sinónimo de 802.11b, ya que éste fue el primer estándar en la familia que disfrutó de un amplia popularidad. Sin embargo, Wi-Fi es el nombre ó término que la industria y particularmente la Alianza Wi-Fi a dado a las redes de área local inalámbricas (WLAN) relacionadas a la familia 802.11 de la IEEE.

Hoy, Wi-Fi puede referirse a cualquier de los tres estándares establecidos: 802.11b, 802.11a y 802.11g, pero solo aquellos que han pasado las pruebas de la Alianza Wi-Fi se les permite referirse como Wi-Fi Certificados.

## I.4.B) 802.11

Ratificado en 1997, 802.11 es el estándar original de esta familia que define reglas de comunicación en redes de área local inalámbrica. Es un estándar abierto de la IEEE que habilita la conexión de alta velocidad de PC's, PDAs y otros dispositivos de comunicación a redes Inalámbricas con Internet. Sin embargo, 802.11 representa un familia entera de especificaciones de la IEEE respecto de las Redes Inalámbricas (WLAN), provee transmisiones de 1 ó 2 MBPS en la banda de los 2.4 GHz, usando espectro extendido con salto de frecuencia (FHSS -Frequency Hopping Spread Spectrum) ó espectro extendido en secuencia directa (DSSS -Direct Sequence Spread Spectrum). Este estándar, actualmente, es obsoleto.

En la Tabla I-4 se muestra la familia completa de los estándares correspondientes al 802.11:

| FAMILIA DE ESTÁNDARES 802.11 | | |
|---|---|---|
| Estándar | Descripción | |
| 802.11a | 54 Mbps | 5 GHz (aprobada 1999) |
| 802.11b | 11 Mbps | 2.4 GHz (1999) |
| 802.11c | Operación de conexiones en puente (movido a 802.1) | |
| 802.11d | Compatibilidad mundial con las regulaciones para uso del espectro de frecuencia inalámbrico (2001). | |
| 802.11e | Soporte para Calidad de Servicio aún en desarrollo y no ratificado. | |
| 802.11f | Protocolo para comunicación entre puntos de acceso de diferentes compañías y para soportar clientes ambulantes (2003). | |
| 802.11g | 54 Mbps standard | 2.4 GHz (2003) |
| 802.11h | Versión ambulante (roaming) de 802.11a para dar soporte a los requerimientos de regulación Europeos en la banda de los 5 Ghz. | |
| 802.11i | Perfeccionamiento a la seguridad de la familia 802.11 (2004). El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras -Seguras- Temporales), y AES (Estándar de Encriptación Avanzado). | |
| 802.11j | Perfeccionamiento a la señalización de los 5 GHz para dar soporte a los requerimientos de regulación del Japón (2004) | |
| 802.11k | Administración de sistema WLAN (en progreso) | |
| 802.11l | Omitida para evitar confusión con 802.11i | |
| 802.11m | Mantenimiento de la documentación de la familia 802.11 | |
| 802.11n | Estándar futuro de 100+ Mbps (en progreso) | |

TABLA I-4. FAMILIA DE ESTÁNDARES 802.11

## I.4.C) 802.11A, 802.11B, 802.11G

Existen tres estándares diferentes para las WLAN (Figura I - 6), desarrollados por la IEEE:

### 802.11A

Se introdujo al mismo tiempo que 802.11b, con la intención de constituirla en la norma para redes inalámbricas para uso empresarial (802.11b se enfocó hacia las redes caseras y para pequeños negocios). Ofrece velocidades de hasta 54 MBPS y opera en la banda de 5 GHz. Su alto precio, el hecho de que la banda de 5 GHz esté regulada en algunos países, y su menor cobertura ha hecho que los equipos 802.11a sean menos populares que los 802.11b.

### 802.11B

Introducido en 1999, como extensión al estándar 802.11 publicado en 1997. Los equipos inalámbricos que operaban con la norma 802.11 nunca llegaron a tener una buena acogida, porque la máxima velocidad de conexión que ofrecían era de 2 MBPS. La norma 802.11b utiliza el método de modulación DSSS (Modulación de Secuencia Directa de Espectro Extendido) usando CCK (Modulación por Cambios de Código Complementarios), que permite una velocidad máxima de 11 Mbps (con un retroceso de 5.5, 2 y 1 Mbps) en la banda de 2.4 GHz con 13 canales disponibles, lo que permitió una funcionalidad wi-fi comparable a Ethernet. El factor de la interferencia es uno de los que más influye, ya que operan en la misma frecuencia que otros equipos como teléfonos inalámbricos, hornos de microondas, etc. A pesar de sus problemas, el estándar 802.11b se ha convertido en el más popular.

### 802.11G

Surgió en 2003, como la evolución del estándar 802.11b. Esta norma ofrece velocidades hasta de 54 MBPS (22 MBPS típicamente) en la banda de 2.4 GHz, y es compatible con los equipos 802.11b, por lo cual ha tenido una gran aceptación, y se prevé que reemplace por completo al estándar 802.11b en un futuro no muy lejano.

**DISTINTAS ESPECIFICACIONES EN WLANs**

| ESTÁNDAR | ESTATUS | MÁXIMA TASA DE BITS | FRECUENCIA DE OPERACIÓN |
|---|---|---|---|
| IEEE 802.11a | Impopular: Menor cobertura, cara y banda regulada. | 54 MBPS | 5 GHz |
| IEEE 802.11b | Utilizado por la mayoría de fabricantes de WLANs | 11 MBPS | 2.4 GHz |
| IEEE 802.11g | Evolución del 802.11b mejorando velocidad y compatibilidad. | 22 - 54 MBPS | 2.4 GHz |
| HiperLAN | Desarrollo por ETSI | 2 MBPS | 5.0 GHz |
| Bluetooth | Promovido por 3Com, Ericsson, IBM, Intel, Microsoft, Motorota, Nokia y Toshiba. | 2 MBPS | 5.0 GHz |

IEEE: Institute of Electrical and Electronic Engineers.
ETSI: European Telecommunications Standards Institute.

TABLA I-5. ESTÁNDARES DE LAS WLANS POR LA IEEE.

## I.5) INCOMPATIBILIDAD, INTERCONECTIVIDAD Y FUTURO DE LAS WLAN´S:

El gran éxito de las WLANs es que utilizan frecuencias de uso libre, es decir no es necesario pedir autorización o algún permiso para utilizarlas. Aunque hay que tener en mente, que la normatividad acerca de la administración del espectro varia de país a país. La desventaja de utilizar este tipo de bandas de frecuencias es que las comunicaciones son propensas a interferencias y errores de transmisión. Estos errores ocasionan que sean reenviados una y otra vez los paquetes de información. Por eso la velocidad máxima especificada teóricamente no es tal en la realidad. Si la especificación IEEE 802.11b nos dice que la velocidad máxima es 11 Mbps, entonces la velocidad máxima de transmisión será aproximadamente 6 Mbps y menos.

Para reducir errores, el 802.11a y el 802.11b automáticamente reducen la velocidad de transmisión. Así por ejemplo, el 802.11b tiene tres velocidades de información (5.5, 2 y 1 Mbps) y el 802.11a tiene 7 (48, 36, 24, 18, 12, 9 y 6 Mbps). La velocidad máxima permisible (Tabla I-5) sólo es disponible en un ambiente libre de interferencia y a muy corta distancia.

La transmisión a mayor velocidad del 802.11a no es la única ventaja con respecto al 802.11b. También utiliza un intervalo de frecuencia más alto de 5 GHz. Esta banda es más ancha y menos saturada que la banda de 2.4 GHz en la que, el 802.11b, comparte con teléfonos inalámbricos, hornos de microondas, dispositivos Bluetooth, etc. Una banda más ancha significa que más canales de radio pueden coexistir sin interferencia.

Por ejemplo: El radioespectro asignado para el 802.11a y el HiperLAN2 es dividido en 8 segmentos o canales de 20 MHz cada uno. Cada canal soporta un cierto número de dispositivos; dispositivos individuales pueden transitar a través de segmentos de red como si fueran teléfonos móviles de una estación a otra. Este espectro de 20 MHz para un segmento de red soporta 54 Mbps de caudal eficaz (throughput) compartido entre los dispositivos en el segmento en un tiempo dado.

Sin bien, la banda de 5 GHz tiene muchas ventajas, también tiene sus problemas. Las diferentes frecuencias y técnicas de propagación que utilizan ambos sistemas (OFDM y DSSS) significa que los productos basados en 802.11a no son compatibles con los 802.11b. Esto significa que aunque no se interfieran entre sí, por estar en diferentes bandas de frecuencias, los dispositivos no pueden comunicarse entre ellos.

Para evitar esto, la IEEE desarrolló un nuevo estándar conocido como 802.11g, el cual extenderá la velocidad y el intervalo de frecuencias del 802.11b para así hacerlo totalmente compatible con los sistemas anteriores. La demora en la ratificación del 802.11g ha obligado a muchos fabricantes irse directamente por el 802.11a donde existe una gran variedad de fabricantes de chips y circuitos integrados tales como Atheros, National Semiconductor, Resonext, Envara, inclusive Cisco Systems quien adquirió a Radiata, la primer compañía en desarrollar un prototipo en 802.11a en el 2000.

Los expertos siguen haciendo énfasis en los problemas inherentes de las tecnologías inalámbricas, tales como las limitaciones de ancho de banda disponible, problemas con interferencia y seguridad de la información transmitida. Sin embargo, muchas de esas barreras que han inhibido el crecimiento de la tecnología inalámbrica están siendo resueltos. Se están superando las cuestiones que giraron alrededor de la estandarización y un número creciente de compañías están ofreciendo una variedad

de soluciones de hardware y software. La propuesta de Atheros[5] es de mejorar esos protocolos y proveer compatibilidad a los productos que cumplan con las especificaciones existentes, además de permitir nuevas capacidades.

Otro aspecto importante de los productos WLAN es la compatibilidad (Tabla I-6). Gracias al desarrollo de estándares pueden interconectarse o mezclarse dispositivos inalámbricos de diversos fabricantes. Aunque hay que mencionar que hay quienes no siguen los estándares y no son compatibles con el resto de los equipos, inclusive de la misma marca.

Al comprar equipo certificado bajo Wi-Fi se protege la inversión al proveer soluciones basadas en estándares. Esto permite hacer compras de diferentes proveedores sin problemas de conectividad o compatibilidad.

| NORMA IEEE / DETALLES | 802.11 | 802.11a | 802.11b | 802.11g |
|---|---|---|---|---|
| FECHA | 1997 | 2000 | 1999 | 2003 |
| FRECUENCIA | 2.4 GHz | 5.8 GHz | 2.4 GHz | 2.4 GHz |
| VELOCIDAD MAX. DE TRANSMISIÓN | 1.2 Mbps | Hasta 54 Mbps | 1, 2, 5.5 y 11 Mbps | Hasta 54 Mbps |
| TECNOLOGÍA | DSSS, FHSS | OFDM | DSSS | OFDM |
| COMPATIBILIDAD | 802.11 | No Compatible 802.11, 802.11b | 802.11 | 802.11b |
| ANCHO DE BANDA | 83 MHz | 150 MHz | | |
| CANALES DE R. F. | 3 | 8 | 3 | 3 |
| COBERTURA | 100 pies a 11Mbps<br>300 pies a 1 Mbps | 40 pies a 54 Mbps<br>300 pies a 6 Mbps | 100 pies a 11Mbps<br>300 pies a 1 Mbps | 50 pies a 54Mbps<br>150 pies a 11Mbps |
| ESTADO | Obsoleta | Poco Auge | La más difundida | Actual |
| | Método de Acceso: CSMA/CA<br>El nodo que va a transmitir debe esperar que el medio esté libre.<br>El receptor del paquete emite un ACK que indica al emisor que no hubo colisión.<br>La comunicación es, en todos los casos, Half Duplex. | | | |
| MÉTODOS DE AUTENTICACIÓN | SISTEMA ABIERTO (OPEN SYSTEM)<br>1) La estación solicitante envía un Pedido de Autenticación con su ID (SSID) | | CLAVE COMPARTIDA - (SHARED KEY)<br>1) Ambas estaciones poseen la misma clave compartida<br>2) La estación envía su clave encriptada en un paquete de "Challenge Text" | |

TABLA I-6. TABLA DE ESTANDARES 802.11

[5] Atheros Comunications, Inc. "Atheros Wireless LAN, 2.4-GHz, 5-GHz, 2.4/5-GHz, 802.11a/b/g, 802.11b/g, 802.11, Radio-on-a-Chip, WLAN, Networking, Home Network". URL: http://www.atheros.com

## I.5. A) UN FUTURO PROMETEDOR PARA LOS CHIPS WLAN

Los equipos de WLANs han abierto nuevos mercados, la demanda continúa abaratándolos dramáticamente. Por ejemplo, las tarjetas de red inalámbrica se pueden conseguir por menos de los $30 dólares, los Puntos de Acceso pueden comprarse por menos de $200 dólares; además muchos incluyen funciones como: enrutamiento, seguridad (firewall), translación de direcciones IP, etc.

A pesar de la crisis económica que atraviesa el mundo, los envíos de chips de WLAN continuarán incrementándose en los próximos años, según un estudio (Figura I-13) de la compañía consultora In-Stat/MDR[6]. En el 2001 se vendieron mundialmente 8 millones de chips con ganancias del orden de $217 millones de dólares, en el 2005 sus ventas fueron de 140 millones de chips y pronostica que en el 2006 se venderán más de 430 millones de chips. Las tecnologías más demandantes serán la IEEE 802.11a y la 802.11g, las cuales ofrecen velocidades de hasta 54 Mbps. El reporte de In-Stat/MDR es el punto de vista de 22 compañías que fabrican chips de WLAN y productos asociados tanto para hogares como para empresas.

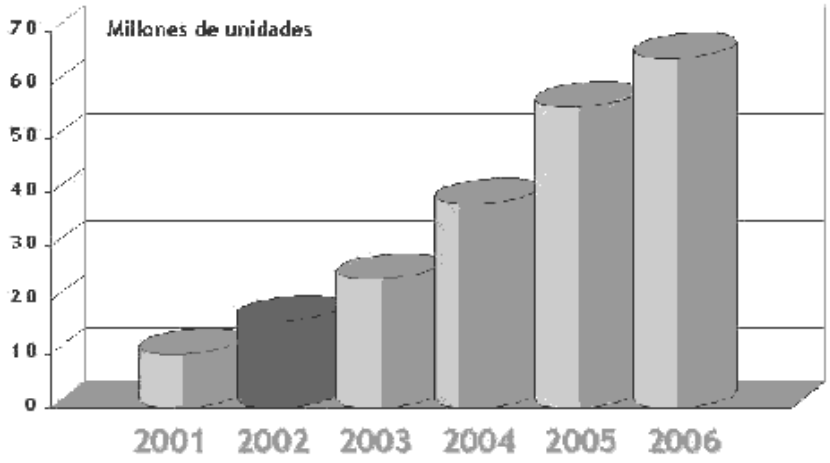



FIGURA I-13. PROYECCIÓN DE VENTAS DE CHIPS INALÁMBRICOS

[6] In-Stat/MDR. "In-Stat - Covering the Full Spectrum of Advanced Communications Market Research". URL: http://www.instat.com

# CAPITULO II

# HISTORIA DE LA SEGURIDAD EN REDES INALÁMBRICAS

# II.1) SEGURIDAD DE LA INFORMACIÓN

## II.1. A) CATEGORÍAS GENERALES DE LA SEGURIDAD INFORMÁTICA

Los objetivos principales de la seguridad informática son garantizar:

**LA CONFIDENCIALIDAD DE LOS DATOS.** Sólo las personas autorizadas deben poder ver la información.

**LA INTEGRIDAD DE LOS DATOS.** Todos los usuarios autorizados deben estar seguros de que los datos que obtienen son precisos y de que no fueron modificados de forma inadecuada.

**LA DISPONIBILIDAD DE LOS DATOS.** Los usuarios autorizados deben poder tener acceso a la información que necesiten, en cualquier momento.

Es un asunto de importancia estratégica, en el cual interactúan la tecnología, los procesos y las personas para definir un esquema real de protección de la información.

La seguridad se puede dividir en seis requisitos o principios. La mayoría de ellos hacen uso de técnicas criptográficas. Éstos principios son igualmente importantes para garantizar la confidencialidad, integridad y disponibilidad de los datos:

**IDENTIFICACIÓN.** La identificación está relacionada con los nombres de los usuarios y con la forma en que éstos se identifican en un sistema informático.

**AUTENTICACIÓN.** La autenticación es todo aquello que tiene que ver con contraseñas, tarjetas inteligentes, biometría, etcétera. Es el método que utilizan los usuarios para demostrar al sistema que son legítimos. Consulte criptosistemas asimétricos en el Anexo E.

**CONTROL DE ACCESO.** Son los privilegios y requerimientos (contraseñas) concedidos a los usuarios para que puedan accesar y realizar determinadas funciones en un sistema informático.

**CONFIDENCIALIDAD.** Garantiza a las personas autorizadas la privacidad de la información y comunicaciones, a través del uso de mecanismos de cifrado o encriptación (Ver Anexo E), para hacer frente a observadores no autorizados.

**INTEGRIDAD.** Abarca aquellos procesos que se ocupan de la prevención y detección de la falsificación, pérdida o daño de los mensajes de datos mientras son transmitidos.

**IMPOSIBILIDAD DE RECHAZO.** Es aquel en el que los datos y solicitudes auténticas sean procesados brindando al cliente el servicio solicitado. Las firmas digitales juegan un papel esencial en este servicio.

## II.1. B) TIPOS DE ATAQUES: PASIVOS Y ACTIVOS

Ataques a la seguridad de las redes son típicamente divididos en ataques pasivos y activos.

### ATAQUES ACTIVOS

Estos ataques son relativamente sencillos de identificar, ya que implican la de modificación del flujo y disponibilidad de datos transmitidos o la creación de un flujo falso de datos, pudiendo subdividirse en cuatro categorías:

1) **La adición**, que se refiere a la introducción de datos al flujo de información.
2) **La modificación**, que implica una alteración a la información original.
3) **La saturación**, inhabilita a un equipo a seguir proporcionando sus servicios (DoS[1]).
4) **La eliminación de los datos** transmitidos, así como registros y archivos completos.

### ATAQUES PASIVOS

En estos ataques están dirigidos a vulnerar la confidencialidad de la información al buscar interceptar el flujo de información sin alterar su contenido, lo cual los hace difíciles de identificar. Un ejemplo es cuando un tercero escucha una conversación telefónica entre dos personas.

Es una técnica muy sutil que puede consistir en:

- **Obtención de información y datos** Si la información no esta encriptada es posible verla.
- **Obtención del origen y destinatario** de la comunicación, leyendo las cabeceras de los paquetes monitoreados.
- **Monitoreo del volumen de tráfico** intercambiado entre las entidades monitoreadas, obteniendo así información acerca de actividad o inactividad inusuales.
- **Monitoreo de las horas habituales** de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

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

El impacto de una mala estratégico de administración de riesgos puede resultar en pérdidas de productividad que afecten al negocio. Si consideramos que una de las aplicaciones más comunes de las redes convergentes es el uso de voz (VoIP[2]) y datos de redes inalámbricas por el mismo canal, el impacto de un ataque DoS sobre el canal de datos implicaría que tanto el sistema de operación transaccional como el telefónico se vieran afectados. ¿Y qué pasaría si la información que corre por la red inalámbrica está expuesta a ser vista por cualquier usuario incluso fuera de nuestras instalaciones?

Cuando las redes proveen el medio de comunicación de voz, multimedia y datos, entre otros, la seguridad se convierte en tema prioritario.

[1] DoS - Negación del Servicio (Denial of Service)
[2] VoIP - Voz sobre IP (Voice over IP)

### II.1.C) MECANISMOS Y FACTORES DE SEGURIDAD

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios de seguridad previamente mencionados. Éstos poseen tres componentes principales:

1) Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.

2) Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.

3) Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una administración de seguridad. La administración comprende dos campos muy amplios:

1) Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.

2) La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

#### FACTORES DE SEGURIDAD

Los factores de seguridad que se definen en un entorno inalámbrico pueden reducirse a cinco elementos básicos:

1. Robo.
2. Control de accesos.
3. Autenticación.
4. Encriptación.
5. Barreras.

## II.2) EL PROBLEMA DE LA SEGURIDAD EN REDES WI-FI

### II.2. A) PROBLEMÁTICA INHERENTE A SU MEDIO DE TRANSMISIÓN

La diferencia principal de los entornos *wireless* con los entornos de cable tradicionales, como *ethernet*, radica en el medio en el que se transmiten los datos.

Algunos de los riesgos son similares a aquellos en las redes cableadas; otros son agravados por la conectividad inalámbrica; varios más, son nuevos.

Sin duda, la fuente más importante de los riegos en redes inalámbricas son *las señales*, que pueden ser escuchadas por intrusos desde fuera de los linderos físicos de una empresa, por ejemplo desde el estacionamiento de la misma. En las redes Wi-Fi, el perímetro de seguridad no está establecido de forma fija, sino que depende del alcance de la señal de radio. Esto obliga a replantear varios conceptos tradicionalmente asociados a la seguridad.

## II.2. B) PUNTOS DE ACCESO MAL CONFIGURADOS

La mala configuración de un punto de acceso inalámbrico es muy común. Es decir, si al adquirir equipo inalámbrico no se cambia la configuración que trae por defecto, sin seguridad alguna, los riesgos que se corren son altísimos ya que el SSID de todos los proveedores son conocidos y ninguna opción de seguridad (WEP o WPA) es habilitada inicialmente.

Un estudio publicado en 2003 por RSA Security Inc.[3] encontró que de 328 puntos de acceso inalámbricos que se detectaron en el centro de Londres, casi las dos terceras partes no tenían habilitado el cifrado mediante WEP (Protocolo de Seguridad Equivalente al Cableado - Wired Equivalent Protocol). Además, cien de estos puntos de acceso estaban divulgando el SSID (Identificador de la red inalámbrica) o información que permitía identificar la empresa a la que pertenecían y 208 tenían la configuración con la que vienen de fábrica, es decir, sin seguridad alguna.

Lo grave de esta situación es que muchos administradores de redes parecen no haberse dado cuenta de las implicaciones negativas de poseer puntos de acceso inalámbrico en la red de una empresa. Es muy común encontrar redes en las que el acceso hacia y desde Internet se protege adecuadamente con un firewall (Ver Glosario) bien configurado, pero al 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 la posibilidad de navegar gratis en Internet, emplear esa red como punto de ataque hacia otras redes y luego desconectarse para no ser detectado, robar software y/o información, introducir virus o software maligno, entre muchas otras cosas. Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la compañía.

## II.2.C) PUNTO DE ACCESO NO AUTORIZADO (ROGUE)

Un punto de acceso no autorizado (rogue) es aquél que ha sido instalado sin la autorización ni el conocimiento de los administradores de red. Por lo cual no esta bajo la administración de los expertos en Tecnologías de la Información ni bajo las políticas de seguridad para la red.

Los puntos de acceso “rogue” son un problema inclusive si la compañía no tiene una red inalámbrica, ya que frecuentemente empleados que buscan mejorar su productividad instalan inocentemente un punto de acceso para su uso personal en la red sin entender los riesgos de seguridad.

Los puntos de acceso rogue son utilizados por hackers para atacar las redes inalámbricas.

[3] RSA Security Inc. “RSA Security: solutions for enterprise data privacy and identity and access management”. URL: http://www.rsasecurity.com

# II.3) ATAQUES PARTICULARES A WI-FI

Esta sección describe algunos ataques, como se ilustra en la Figura II-1, específicos a las redes inalámbricas que representan riesgos significativos. Con la variedad de herramientas ampliamente disponibles en Internet, libros y revistas, un hacker novato puede ejecutar una multitud de ataques como si fueran recetas de cocina.

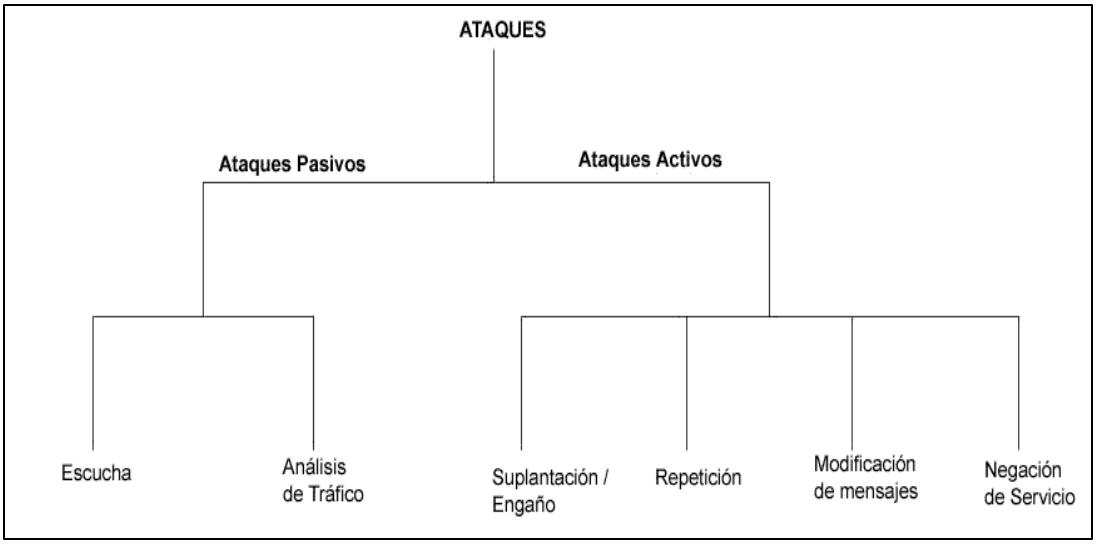



FIGURA II - 1. ATAQUES PARTICULARES A WI-FI

## II.3.A) ATAQUES PASIVOS

### ESPIONAJE: ESCUCHA Y MONITOREO

Las redes inalámbricas son especialmente vulnerables a los ataques pasivos, ya que el único requisito para su realización es estar en su área de cobertura (Vea la sección III.1.B).

El primer paso es conseguir una asociación con la red inalámbrica. En las redes que utilizan autenticación abierta o nula (*Open System)*, el proceso es transparente, aumentando su complejidad en los sistemas con autenticación *Shared Key*. En estos casos, la autenticación es posible tras la captura de cierto número de paquetes para develar *(cracking)* la clave, existiendo diversas herramientas que facilitan dicha tarea (Vease Anexo C).

Tras ello, es posible obtener datos, información, direcciones MAC de los equipos origen y destino, direcciones IP, horario de uso, volumen y monitoreo del tráfico que esta presente en el entorno inalámbrico.

En otras palabras, se realiza el espionaje al escuchar todo lo que se transmite durante y dentro del canal de comunicaciones.

Como ya se menciono, los ataques pasivos son muy difíciles de detectar ya que no alteran los datos.

La implementación práctica de los ataques de escucha se conoce como *wardriving.*

## II.3.B) ATAQUES ACTIVOS

Son ataques en los cuales se lleva a cabo la modificación de los mensajes, paquetes o archivos.

**SUPLANTACION.** El atacante personifica un usuario autorizado y por lo tanto obtiene privilegios no autorizados.

**REPETICION (REPLAY).** El atacante monitorea las transmisiones y retransmite mensajes como un usuario legitimo.

**MODIFICACION DE MENSAJES.** El atacante altera un mensaje legitimo al borrarlo, agregarlo, cambiarlo o reordenándolo.

**NEGACION DE SERVICIO (DoS).** Un ataque de negación de servicio, DoS (Denial of Service), es un ataque que impide a la víctima usar total o parcialmente los servicios o comunicaciones de su red.

Este tipo de ataque puede estar dirigido a:

- Un usuario, para impedirle realizar conexiones salientes de la red.
- Una organización completa, para detener su tráfico saliente o entrante a ciertos servicios de red, tales como las páginas de Web de la organización.

Los ataques DoS son más fáciles de realizar que obtener, remotamente, acceso administrativo a un sistema. Debido a esto, un ataque DoS se ha convertido en algo común en Internet.

Existen varias herramientas gratuitas y amigables tales como Wireless LANJack y Hunter_killer (Vea Anexo F) que pueden lanzar ataques de negación de servicio. Los ataques DoS, pueden estar dirigidos contra una máquina en específico para evitar que esta se comunique con la red, contra un punto de acceso para prevenir que las estaciones de trabajo se conecten con éste o contra todos los dispositivos de la red. En este caso, el ataque termina con toda la actividad de la red inalámbrica.

Por las características propias del medio, es sencillo realizar ataques que afecten a la disponibilidad de la información en los entornos inalámbricos. Dichos ataques pueden ser abordados desde varios enfoques, siendo los más sencillos aquellos que utilizan un dispositivo de radiofrecuencia (RF) de alta potencia para generar interferencias, por ejemplo un horno de microondas, lo que prevendría que el usuario legítimo pudiera utilizar el servicio. Esto es consecuencia de la implementación de la capa MAC de 802.11b, que no transmitirá mientras detecte otra actividad de RF. Para evitar las colisiones inherentes al protocolo CSMA/CA, el estándar utiliza paquetes para reserva de tiempo (RTS) a los que el AP contesta (CTS), obligando al resto de estaciones a no transmitir durante el intervalo definido en CTS. Enviar paquetes falsos de RTS generaría una red lenta o inoperable.

La página de Web, no oficial, de seguridad 802. 11 en http://www.drizzle.com/~aboba/IEEE hace un listado de los ataques de Negación de Servicio (DoS) que son lanzados al manipular estaciones inalámbricas, operando EAP y puntos de acceso con comandos de inicio, mensajes prematuros de conexión exitosa, mensajes de falla y otras modificaciones de EAP.

### TIPOS DE ATAQUES DOS

Existen unos cuantos ataques DoS clásicos. La mayoría se basan en las debilidades del protocolo TCP/IP. Las mejoras de los fabricantes y una configuración apropiada de red han hecho que los ataques DoS sean difíciles o imposibles de realizar.

A continuación se describen en la Tabla II-1 algunos de los ataques DoS:

| TIPO DE ATAQUE DOS | DESCRIPCION |
|---|---|
| **INUNDACIÓN (FLOOD)** | Es el más antiguo de los ataques DoS. El atacante simplemente envía más tráfico que el que la victima puede soportar. Esto requiere que el atacante tenga una conexión de red más rápida que la víctima. Este es el menos sofisticado, tecnológicamente, de los ataques de negación de servicio y también el más difícil de prevenir completamente. |
| **TOQUE DE LA MUERTE (PING OF DEATH)** | Se basaba en un error de la pila de los protocolos TCP-IP de Berkley, el cual también existía en la mayoría de los sistemas que copiaron el código de la Universidad de Berkeley. El toque de la muerte simplemente enviaba paquetes de sondeo mayores de 65,535 bytes a la víctima.<br>Esto era tan simple como: ping -l 86600 vicitm.org |
| **SINCRONÍA (SYN)** | En el protocolo TCP/IP, el enlace de conexión de red es realizado con mensajes SYN y ACK. El sistema que desea comunicarse envía un mensaje de solicitud, SYN, al sistema destino. El sistema destino responde con un mensaje ACK. En un ataque SYN, el atacante inunda al destinatario con mensajes SYN engañosos para aparecer estar en una dirección de Internet inalcanzable. Esto llena y sobrepasa el espacio para mensajes SYN en el equipo destino, impidiendo que otros sistemas de la red puedan comunicarse con éste. |
| **BLOQUEO (TEARDROP)** | Utiliza el algoritmo de fragmentación de los paquetes IP para enviar paquetes dañados a la máquina de la víctima. Esto, la confunde y puede bloquearse. |
| **(SMURF)** | El atacante envía una solicitud de contestación (ping) a una dirección de emisión masiva (broadcast) desde otro equipo en la red. Esta solicitud es modificada para hacerla parecer que viene de la dirección de red de la victima. Cada equipo, dentro del dominio de emisión de esa red, enviara una respuesta a la víctima. |
| **DOS DISTRIBUIDO (DDOS)** | Un ataque de negación de servicio distribuido, es un ataque DoS ejecutado desde una gran cantidad de sitios, que han sido comprometidos por un gusano, caballo de Troya o por un hacker manualmente.<br><br>Esos equipos comprometidos son usualmente controlados con un software sofisticado cliente servidor tal como Trinoo, Tribe Flood Network, Stacheldaht, TFN2K, Shaft y Mstream.<br><br>El gusano Mydoom intento ataques DDoS contra las compañías Microsoft y SCO desde los sistemas que infecto.<br><br>Puede ser muy difícil defenderse y combatir ataques DDoS. |

TABLA II-1. ATAQUES DOS

## II.3.c) ATAQUES AVANZADOS

Algunos ataques implementados a partir de las modalidades mencionadas son:

## ATAQUE DE DICCIONARIO

Ataque de diccionario es aquel en el se intenta cada palabra de un diccionario como posible password de un mensaje encriptado. Este tipo de ataque es mas eficiente que el de fuerza bruta, ya que los usuarios típicamente utilizan password pobres o muy sencillos.

Existen dos métodos para mejorar los ataques de diccionario:

1) El primero consiste en usar un diccionario mas grande o usar mas diccionarios.
2) El segundo consiste en ejecutar una manipulación de las palabras del diccionario. Por ejemplo la palabra "password" puede estar en el diccionario, y con técnicas para manipularlo se puede invertir (drowssap), adicionar combinaciones de números y letras (p4ssw0d) o usar mayúsculas (Password).

Otra opción es usar una lista de nombres de mujeres.

Un pequeño diccionario puede tener resultados sorprendentes con estas técnicas.

## ATAQUE DE FUERZA BRUTA

Un ataque de fuerza bruta consiste en intentar todos las posibles claves, códigos, combinaciones o contraseñas hasta encontrar el correcto. La dificultad de estos ataques depende de varios factores:

¿Que tan larga puede ser la clave?
¿Cuantos valores posibles pueda cada componente de la llave tener?
¿Cuanto tiempo tomará intentar cada clave?

Por ejemplo, imagine un sistema en el cual permite solo 4 dígitos (PIN). Esto significa que el máximo de combinaciones posibles son 10,0000.

**INCREMENTANDO LA SEGURIDAD CONTRA ATAQUES DE FUERA BRUTA**

Del ejemplo anterior, la seguridad del PIN puede ser incrementada al:

- Incrementar la longitud del PIN
- Permitir que el PIN contenga otros caracteres además de números, tal como * o #
- Implantar un retraso de 30 segundos entre intentos de autenticación fallidos.
- Bloquear la cuenta después de 5 intentos fallidos.

Un ataque de fuerza tendrá éxito, eventualmente. Sin embargo, ataques de fuerza bruta contra sistemas con llaves suficientemente largas requerirán billones de años en completarse.

En muchos casos un ataque de diccionario trabajará mas rápidamente que un ataque de fuerza bruta. Pero un ataque de fuerza bruta es, sin embargo, mas seguro de lograr resultados eventualmente que un ataque de diccionario.

## ASOCIACIÓN MALIGNA O ACCIDENTAL

Un hacker puede forzar a una estación de trabajo a conectarse, sin que ésta lo sospeche, a un red 802.11no deseada o ficticia, o alterar la configuración de la estación para operar en modo de red ad-hoc. Para empezar, los hacker configuran una computadora portátil como un punto de acceso "suave" usando cualquiera de las herramientas gratuitas (Anexo F) para hacker tales como HostAP, Airsnarf o Hotspotter, o alguna herramienta comercialmente disponible. (Compañías tales como PCTel proveen software comercial que convierte dispositivos 802. 11 en puntos de acceso).

Así pues cuando la estación de trabajo de la victima transmite una solicitud para asociarse con un punto de acceso, el punto de acceso suave del hacker responde a esta petición y establece una conexión entre los dos. A continuación el punto de acceso suave provee una dirección IP a la estación de trabajo de la víctima. Una vez hecho esto, el hacker puede escudriñar la estación de la víctima con herramientas diseñadas para encontrar vulnerabilidades bajo Windows. El hacker puede entonces robar información, instalar gusanos, troyanos u otros programas de espionaje (spyware) y si está conectada a una red cableada, usan la estación de la víctima como una plataforma de lanzamiento para obtener acceso a otros servidores.

Las Redes Inalámbricas están sujetas a la distracción. Las estaciones no siempre saben a cuales puntos de acceso o redes se están conectando. Las estaciones pueden ser engañadas o forzadas para conectarse a puntos de acceso maliciosos, ya que frecuentemente no hay autenticación en el punto de acceso. Esto es un una vulnerabilidad a nivel capa dos (Enlace de Datos).La autenticación a nivel capa 3 (Red) no ofrece ninguna protección contra ello, tampoco lo hace el uso de redes privadas virtuales (VPNs).

WLANs con autenticación basada en 802.1X (capa 2) ayuda a proteger contra asociaciones maliciosas, pero son vulnerables.

Un ataque de asociación maliciosa no trata de irrumpir la VPN u otras medidas de seguridad. En su lugar, toman posesión del cliente a nivel capa 2.

## ROBO DE IDENTIDAD (MAC SPOOFING)

El robo de la identidad de un usuario autorizado es una amenaza seria para las redes inalámbricas. Aún cuando el SSID y las direcciones MAC actúan como un número de identificación personal (PIN) al verificar la identidad de los clientes autorizados, los estándares de encriptación no son una garantía. Los hacker con conocimientos pueden elegir direcciones MAC o SSID autorizadas y robar ancho de banda, bajar archivos o dañarlos y ejecutar la destrucción de la red entera.

Algunas compañías aseguran sus redes inalámbricas al usar una lista de direcciones MAC de los equipos autorizados como autenticación. Mientras que este método provee alguna seguridad para instalaciones pequeñas, las direcciones MAC nunca fueron diseñadas para este uso.

Aún si se utiliza encriptación o VPNs, las direcciones MAC están siempre en el aire. Con algunas herramientas de software tal como Kismet o Etherreal, un hacker puede fácilmente capturar la dirección MAC de un usuario válido. Para llevar a cabo el robo de identidad, un hacker puede cambiar su dirección MAC por la de su víctima, usando un programa diseñado para esto, como SMAC, o manualmente, cambiar el registro en Windows. Una vez que esto ha sido hecho, el hacker puede conectarse la red inalámbrica, rebasando cualquier filtrado de direcciones MAC.

Existe la idea falsa de que el robo de identidad es posible solamente si la dirección MAC es usada para autenticación y que los esquemas de autenticación basados en 802.1X son totalmente seguros. Rompiendo LEAP para robar la identidad se ha vuelto fácil con herramientas tales como ASLEAP y THC-LeapCracker. Otros esquemas de autenticación, tales como EAP-TLS y PEAP, pueden requerir ataques más sofisticados que exploten otras vulnerabilidades conocidas en la parte cableada de los esquemas de autenticación, pero son factibles.

El monitoreo de radiofrecuencia permite garantizar a los usuarios que la autenticación apropiada está siendo impuesta y cumplida. Adicionalmente, intentos de autenticación excesiva pueden indicar intentos maliciosos de un hacker.

## ATAQUE DE HOMBRE EN MEDIO

Uno de los ataques más sofisticados, es el ataque del hombre en medio. Rompe las conexiones entre las estaciones autorizadas y los puntos de acceso al insertar una estación malévola entre la víctima y el punto de acceso, convirtiendo al hacker en el "hombre en medio".

Éstos ataques son similares a los ataques efectuados en redes cableadas, y las herramientas para realizar esos ataques en redes cableadas pueden ser usados en redes inalámbricas. Entrar en medio de una sesión de comunicaciones es un problema en redes cableadas. Este proceso es mucho más fácil en las redes inalámbricas ya que una estación que transmite no es capaz de detectar la presencia de estaciones con la misma dirección MAC o IP. Usando software SoftAP, un hacker puede fácilmente convertir un dispositivo inalámbrico en un punto de acceso suave y posicionar el punto de acceso en medio de la sesión de comunicación.

El ataque de hombre en medio más sofisticado roba al protocolo de saludo y desafío para ejecutar un ataque de des-autenticación. Éste ataque expulsa a un usuario de un punto de acceso, ocasionando que ese usuario busque otro punto de acceso al cual conectarse. Con el punto de acceso, SoftAP, del hacker funcionando, el usuarios se reconecta a la computadora portátil del hacker.

Ahora el hacker con una interfase inalámbrica diferente, se conecta a la red inalámbrica real, pasando todo el trafico de autenticación a través de él. La víctima es ajena a todos esto, y pasa todos los datos a través del equipo del hacker. Este escenario es posible ya que las VPNs establecen sus conexión en la capa 3 del modelo OSI, mientras que las redes inalámbricas existen debajo de las VPN, en las Capas 1 y 2.

Una vez conectado, el hacker puede usar herramientas tales como DSNIFF, Ettercap, IKEcrack u otras herramientas para revertir la seguridad de la VPN hasta que el tráfico este en texto o este usando una encriptación débil de fácil rompimiento. Este es un problema común para la mayoría de los protocolos de VPNs, tales como IPSEC, PPTP, SSH, SSL y L2TP.

Adicionalmente, herramientas gratuitas, incluidas AirJack y LANJack, habilitan a los hackers para el lanzamiento de ataques de hombre en medio al automatizar los pasos para ejecutarlos.

Solo un sistema de detección de intrusos altamente capaz y que monitoree las 24 hrs. Puede detectar esos tipos de ataques en redes inalámbricas. Una solución de seguridad efectiva mantiene bajo observación constante a la red, mientras simultáneamente analiza la actividad del tráfico. Ya que este

tipo de ataque no esta basado en una firma particular, un sistema IDS inalámbrico debe ser capaz de correlacionar y analizar datos para mostrar que este tipo de ataques esta sucediendo.

## ATAQUE DE INJECCION DE TRÁFICO A LA RED

Es un nuevo desarrollo de negación de servicio (DoS), éste ataque explota dispositivos inalámbricos mal configurados y su objetivo es la red entera. Cuando un punto de acceso es conectado a una sección no filtrada de la red corporativa, emite tráfico de red, tal como "Spanning Tree" (802.1D), OSPF, RIP, HSRP y otro tráfico dirigido o diseminado (multicast y broadcast respectivamente). Al hacer esto los paquetes incitan ataques que derriban los equipos de las redes inalámbricas y cableadas e impulsan a disolver la infraestructura entera de la red interna, incluidos los hubs, ruteadores y switches.

El algoritmo "Spanning Tree" normalmente asegura una topología libre de loops[4] para redes que contienen puentes paralelos y segmentos Ethernet múltiples.

Los loops ocurren cuando hay rutas alternas entre los clientes (hosts). Si existe un loop en una red extensa, los puentes podrían enviar tráfico a hosts Ethernet falsos o erróneos indefinidamente, incrementando el tráfico y reducir el rendimiento de la red al punto donde la red para de responder. Un hacker puede inyectar tráfico sobre el segmento de red inalámbrica y será propagado a través de la red completa. Esto crea un ataque de DoS al insertar intencionalmente loops dentro de la red.

Sniffers bribones inician el ataque de DoS al repetir sesiones de "Spanning Tree" manipuladas detrás del punto de acceso de la red inalámbrica. El punto de acceso repite los paquetes a otro host interno, causando un efecto domino. Los ataques de Spanning Tree usualmente hacen inoperables hubs inteligentes, puentes y switches, requiriendo que los dispositivos sean re-inicializados o reconfigurados para hacerlos funcionales nuevamente.

Ataques de ruteo son otros ataques de moda DoS. Un hacker puede utilizar herramientas tales como IRPAS o Routing Atack Tool para inyectar actualizaciones de ruteo falsas dentro de la red, cambiando la puerta (gateway) por defecto o destruyendo las tablas de ruteo. Cualquier punto de acceso falso en la red que no esta filtrado por una puerta abre la red a este ataque dañino. Se ha descubierto que una de cada cinco redes corporativas son vulnerables a este tipo de ataque.

### OTRO TIPO DE ACTIVIDADES

Cabe también mencionar la utilización de computadoras conectadas a Internet cuyo nivel de procesamiento y de seguridad son bajos. Éstas son usadas en conjunto (por software de spyware o gusanos) para:

- Atacar - Ataque distribuido de negación de servicio (DDoS)
- Romper llaves de seguridad.
- Decodificar algoritmos de seguridad.

[4] Loops - ciclos infinitos, ir en círculos.

# II.4) EVOLUCIÓN DE LA SEGURIDAD EN REDES 802.11

802.11 inicia con un mecanismo llamado WEP cuyas fallas hacen que la Alianza WiFi desarrolle un conjunto temporal de soluciones denominadas WPA. Las cuales resuelven los requerimientos inmediatos de la industria. El IEEE seguía trabajando en su estándar 802.11i y ante su lentitud se consolida la segunda versión temporal de seguridad: WPA2, la cual incluye más elementos de seguridad como encriptación AES que demanda mayor capacidad de procesamiento, por lo cual se requiere de equipo nuevo.

Tanto WPA, como WPA2 no son estándares "per se". Sin embargo como han sido la solución temporal mientras se desarrollaba el estándar de la IEE, se les trata como tales.

Finalmente ve la luz la solución planteada por el IEEE el tan esperado estándar 802.11i, después de 3 borradores y casi cuatro años de diseño. Éste se basa en todos los adelantos logrados por WPA2 pero hace obligatorios varios elementos que en WPA2 son solo opcionales.

A modo de un rápido recorrido, se muestra la Figura II-2 donde se observa la evolución de dichos estándares.

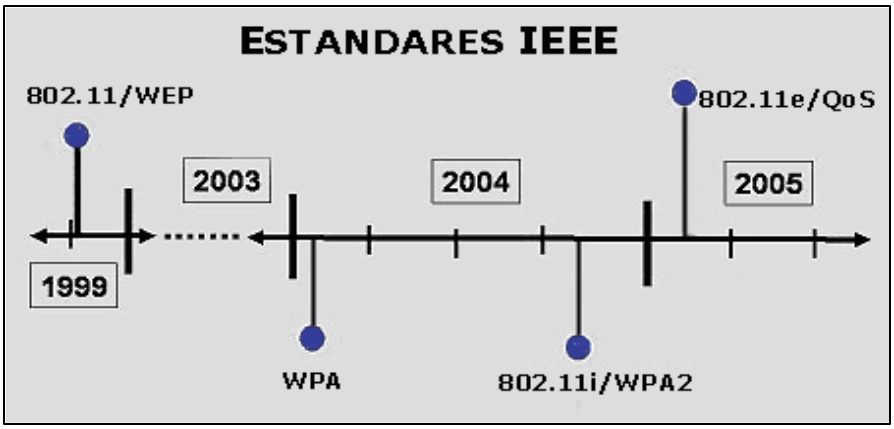



FIGURA II-2. EVOLUCIÓN DE LOS ESTÁNDARES DE SEGURIDAD DEL IEEE

Veremos la evolución de la seguridad para redes inalámbricas en detalle en este capítulo.

## II.4. A) REQUERIMIENTOS PARA TENER UNA RED INALÁMBRICA SEGURA

Los organismos de estándares, incluyendo el IEEE, el IETF y la Alianza WiFi han definido tres áreas básicas de seguridad para tener una red inalámbrica segura:

1) **AUTENTICACIÓN**. Método que certifica, válida y controla el acceso de los usuarios y dispositivos a la red.

2) **CONFIDENCIALIDAD**. Para brindar privacidad los comunicaciones se encriptan. Sinónimo de métodos de encriptación (WEP, TKIP, AES)

3) **INTEGRIDAD**. Aquellos procesos que prevén y detectan la falsificación de los mensajes de datos. Los paquetes transmitidos deben estar originados por los emisores.

El objetivo de estos servicios es el de ofrecer seguridad, bajo cualquier circunstancia.. Para lograrlo se han desarrollado varios estándares, métodos y algoritmos de seguridad.

## II.4. B) WEP

El primer mecanismo de seguridad, WEP[5], **(**Privacidad Equivalente al Cableado - Wired Equivalent Privacy) inicia con las WLANs en 1999. Desarrollado por voluntarios del IEEE[6] cuyo objetivo era brindar seguridad a las redes inalámbricas al proveer: *Integridad, Confidencialidad y Autenticación.*

Poco tiempo después de salir al mercado este mecanismo, e inclusive desde antes, ya mostraba serias fallas de seguridad. La Figura II-3 permite observar cuando fueron localizadas sus vulnerabilidades. Estudios de la Universidad de California - Berkley, Universidad de Maryland- Collage Park y la Universidad de Helsinki detallaron las numerosas deficiencias de seguridad de WEP. Software gratuito, que puede descargarse de Internet, permite que ataques automatizados sobre WEP puedan ser llevados a cabo con facilidad.

En agosto del 2001, Stubblefield, Ioannidis y Rubin implementaron un sistema práctico y sencillo para conseguir la clave con la vulnerabilidad del RC4. Consiguieron la clave en 2 tipos de experimentos con:

- Entre 5 y 6 millones de paquetes utilizando sólo la vulnerabilidad.
- Sobre 1 millón de paquetes combinando esta técnica con otras.

Los programas gratuitos Airsnort y WEPCrack utilizan esta técnica.

| Fecha | Descripción |
|---|---|
| Septiembre 1995 | Vulnerabilidad RC4 potencial (Wagner) |
| Octubre 2000 | Primera publicación sobre las debilidades de WEP: *Insegura para cualquier tamaño de clave; Análisis de la encapsulación WEP* (Walker) |
| Mayo 2001 | Ataque contra WEP/WEP2 de Arbaugh |
| Julio 2001 | Ataque CRC *bit flipping – Intercepting Mobile Communications: The Insecurity of 802.11* (Borisov, Goldberg, Wagner) |
| Agosto 2001 | Ataques FMS – Debilidades en el algoritmo de programación de RC4 (Fluhrer, Mantin, Shamir) |
| Agosto 2001 | Publicación de AirSnort |
| Febrero 2002 | Ataques FMS optimizados por h1kari |
| Agosto 2004 | Ataques KoreK (IVs únicos) – publicación de chopchop y chopper |
| Julio/ Agosto 2004 | Publicación de Aircrack (Devine) y WepLab (Sánchez), poniendo en práctica los ataques KoreK. |

FIGURA II-3. CRONOLOGÍA DE VULNERABILIDADES WEP

### INTEGRIDAD EN WEP

Se aplica un algoritmo de comprobación de integridad (CRC-32) a los datos a transmitir, lo que genera un valor de integridad (ICV[7]). El ICV y los datos se depositan en paquete que se envía al receptor. El receptor ejecuta el mismo algoritmo sobre los datos del paquete recibido y compara su resultado con el ICV que recibió como parte del paquete. Sin ambos ICV son iguales el mensaje será considerado como integro, de lo contrario, el paquete y por ende los datos han sido alterados.

Es fácil observar que este mecanismo no es a prueba de colisiones ni de ataques, ya que se puede llegar el mismo valor de ICV con diferentes datos dentro del paquete transmitido.

[5] Borisov, Nikita. Goldberg, Ian. Wagner, David. "Security of the WEP algorithm". February 02, 2001. URL: http://www.isaac.cs.berkley.edu/issac/wep-faq.html
[6] *Authentication and Privacy*. "An ANSI / IEEE Standard 802.11". 1999. URL: http://standards.ieee.org/getieee802/download/802.11-1999.pdf
[7] Valor para Verificar la Integridad (ICV - *Integrity Check Value)* de 32 bits de longitud.

## CONFIDENCIALIDAD EN WEP

Se logra al habilitar WEP y se configura una clave secreta en cada una de las estaciones y puntos de acceso del sistema WLAN. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el *desafío (challenge)*. La estación debe utilizar su clave secreta para cifrar el texto de desafío y devolverlo -cifrado- al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando su clave y compara con el texto de desafío original que envió. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. De lo contrario, el punto de acceso la rechaza, evitando que la estación acceda a la red.

Si WEP esta deshabilitado (Figura II-4) todos los datos transmitidos viajan sin ningún método de encriptación, es decir, en texto normal. La utilización de WEP es *opcional.* Pero de ser habilitada la velocidad de las transmisiones se deterioran notablemente.

## AUTENTICACIÓN EN WEP

Como se muestra en la Figura II-4 existen dos tipos de autenticación:

**SIN ENCRIPTACIÓN O AUTENTICACIÓN ABIERTA (OPEN SYSTEM)** - No se requiere de absolutamente ninguna configuración especial. El cliente solicita acceso a la red ofreciendo su SSID y su dirección MAC para ser identificada. Si el SSID es igual al del punto de acceso obtiene una dirección IP, con la cual se comunicarse a partir de este momento.

**ENCRIPTADA O DE CLAVE COMPARTIDA (SHARED KEY)** Se requiere habilitar la opción WEP y configurar todos los dispositivos inalámbricos con la misma clave, manualmente, siendo ésta guardada en su chip de configuración. El cliente transmite y recibe, encriptando y desencriptando, todas sus comunicaciones con dicha clave.

Como se puede apreciar la autenticación era opcional y muy débil en WEP.

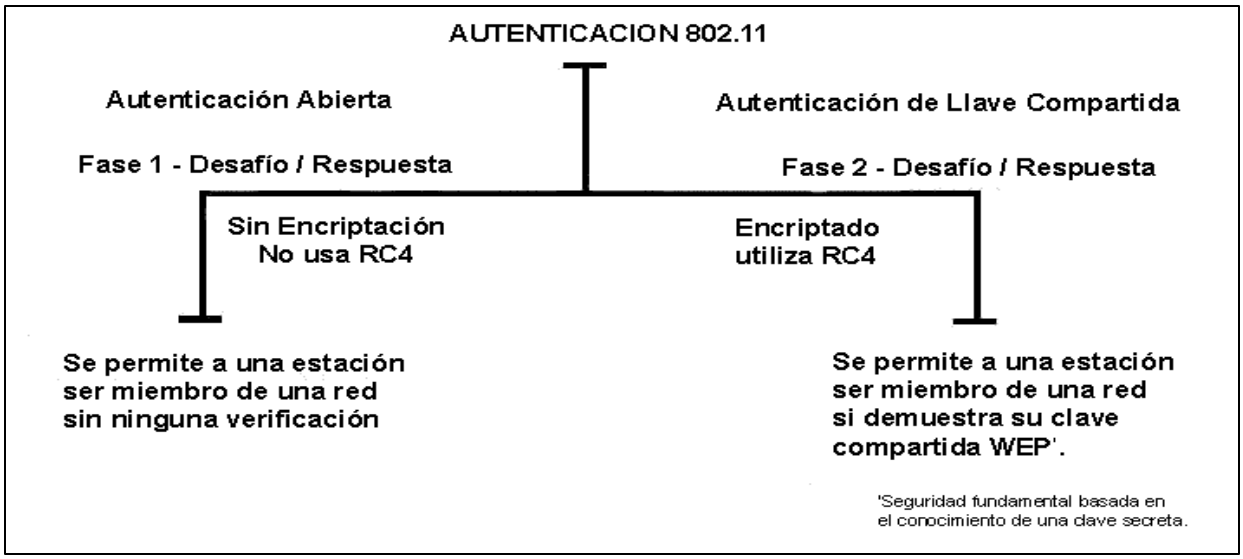



FIGURA II-4. TIPOS DE AUTENTICACIÓN PARA REDES INALÁMBRICAS 802.11/A/B.

# II.4.B. I) MECÁNICA DE ENCRIPTACIÓN / DESENCRIPTACIÓN DE WEP

## ELEMENTOS DE CIFRADO WEP

VI = Vector de Inicialización de 24 bits. Cuyo rango va de 0 a $2^{24}$ = 16,777,215. Cíclico o estático.
C = Clave secreta de 40 bits o 64 bits, conocida en todos los dispositivos. WEP2 utilizó 128 bits.
RC4 = Mecanismo de encriptación. CRC32 = Algoritmo para verificar la Integridad de los datos
T = Texto a transmitir

## PASOS PARA CIFRAR:

1) Se obtiene el ICV[5] al calcular el CRC32 de los datos a transmitir. ICV = CRC32(T)
2) Se forma la semilla (*seed* ) Z al concatenar C y VI. Z = C + VI.
3) Se ejecuta el RC4 sobre Z. Se obtiene (K), el *Keystream*. K = RC4(Z).
4) Se ejecuta el método Xor[8] sobre el ICV y K. Se obtiene (TC), Texto Cifrado. TC = Xor (ICV, K).
5) Se forma el paquete a enviar: VI + TC. El *VI viaja sin cifrar*. P = IV+TC.

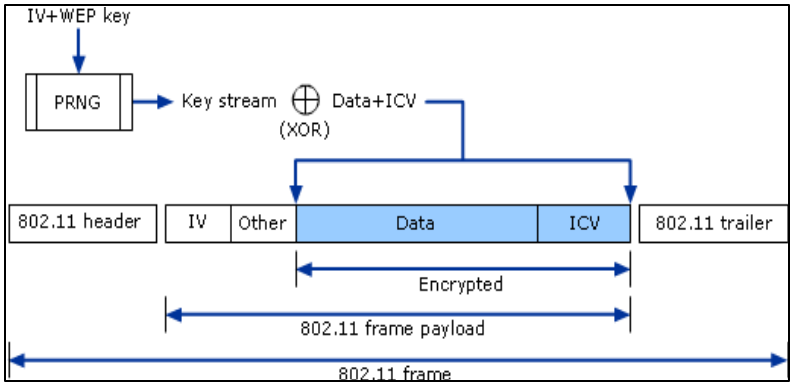



FIGURA II-5. CIFRADO DE WEP

## PASOS PARA DESCIFRAR

1) Se recibe el paquete que contiene el VI el Texto Cifrado. P = VI + TC
2) Se general la semilla ya que se conoce el VI y la Clave Secreta compartida. Z = C + VI
3) Se aplica el RC4 sobre la semilla para obtener el *Keystream*. K = RC4(Z)
4) Se ejecuta el Xor a K y los datos recibidos (TC), se obtiene el Texto original (T). T = Xor (TC, K).

El Keystream actúa como una máscara o valor constante para ejecutar el Xor y así "cifrar" y "descifrar" la información. El VI viaja sin cifrar y es cíclico o fijo, es decir es visible y se repite. Lo que hay que esperar es que al hacer el Xor entre el Keystream y texto cifrado se obtenga el mismo resultado. De hacerlo se habrá encontrado la clave secreta (C).

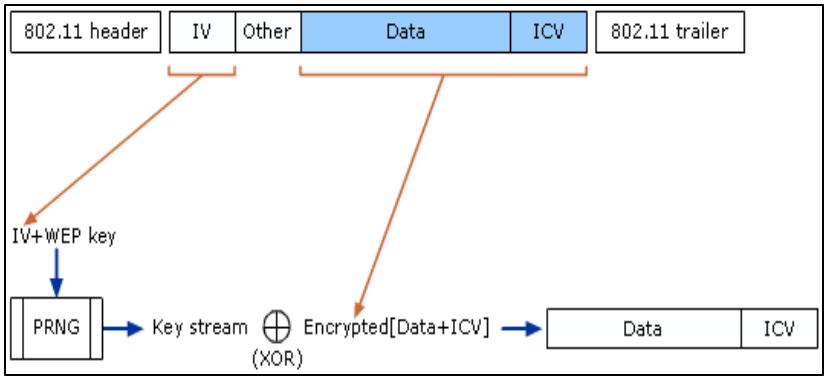



FIGURA II-6. DESCIFRADO DE WEP.

[8] Algoritmo binario con la siguiente lógica a nivel de bis: 0 (Xor) 0 = 0, 0 Xor 1 = 1, 1 Xor 0 = 1 y 1 Xor 1 = 0.
Al hacer un Xor a dos valores y a cuyo resultado aplicamos otro Xor respecto de uno de los valores originales, obtenemos el otro valor original. El Xor (Xor (X, Y), X) obtiene Y. El Xor (Xor (X, Y), Y) obtiene X.
Ejemplo: X=01001101, Y=11010111. El Xor(X, Y) =10011010 = Z.
Finalmente, Xor(Z, X) = (10011010 Xor 01001101) = 11010111, el cual es Y.

## II.4.B. II) VULNERABILIDADES DE WEP

1. Clave WEP estática - Se usa la misma clave WEP en todos los dispositivos.

2. Vector de Inicialización (VI) de 24 bits - Los valores van desde 0 hasta $2^{24}$ = 16,777,215. Es un número que se incrementa por cada paquete enviado para encriptar los datos. En una red con tráfico se reiniciará en forma cíclica y el valor del VI se repetirá. Al seleccionar los VI repetidos de la cadena de datos, un atacante pude coleccionar suficientes datos para averiguar la clave WEP. Adicionalmente este valor es transmitido como texto sin cifrar.

3. Programas gratuitos, de fácil manejo, que pueden recuperar la clave WEP.

4. Desencriptación no autorizada y la violación de la seguridad de los datos - Una vez que la clave WEP es revelada, un hacker puede transformar el texto cifrado a su forma original y entender los datos. Al entender el algoritmo, un hacker puede usar la clave WEP obtenida para modificar el texto cifrado y reenviar un mensaje modificado al receptor. Exponiendo con esto a la red inalámbrica a ataques pasivos y activos.

5. Administración pobre de la clave - Una clave de WEP es tecleada manualmente en cada dispositivo inalámbrico para habilitar WEP. Desafortunadamente, no existen mecanismos para renovar la clave WEP. Una vez que la clave de WEP esta en riesgo, por ejemplo, un empleado deja la compañía; la clave tiene que ser cambiada -manualmente- para mantener la seguridad. El cambio de claves puede ser aplicable en un ambiente casero o en un pequeño negocio. Sin embargo, en un ambiente empresarial con cientos de dispositivos móviles esta tarea se convierte en una misión casi imposible[9].

6. Punto de Acceso sin Autenticación - WEP solamente provee un método para que las tarjetas de red autentiquen puntos de acceso. No existe forma para que los puntos de acceso autentiquen a las tarjetas de red. Como resultado, es posible para un hacker enviar los datos a puntos de acceso a través de una ruta alterna no autorizada, por ejemplo, un punto de acceso instalado por un hacker.

7. WEP no era activado por defecto, cuando estaba disponible.

La industria no podía esperar al estándar 802.11i hasta fines del 2003 (como se esperaba y ahora sabemos que fue hasta el 2004). Se estaba demandando un ambiente inalámbrico más seguro inmediatamente. En respuesta, la Alianza Wi-Fi, junto con la IEEE, desarrolló el WPA (Wi-Fi Protected Access - Acceso Protegido Wi-Fi), en un esfuerzo por atender las vulnerabilidades de WEP y ofrecer un estándar de seguridad fuerte e interoperable al mercado en el primer cuatrimestre del 2003.

[9] Dismukes, Trey "Azariah", "Ars Technica: Wireless Security Blackpaper". July 2002. URL: http://www.arstechnica.com/paedia/w/wireless/security-1.html

## II.4.c) WPA: ACCESO PROTEGIDO WI-FI

WPA es el acrónimo de Wi-Fi Protected Access, es decir, Acceso Protegido para Redes Inalámbricas. Presentado en abril del 2004 por la Alianza Wi-Fi en la ciudad de Las Vegas durante el evento Network+ Interop. WPA es una solución de seguridad temporal cuyo objetivo es resolver todas las vulnerabilidades de WEP. Mientras no estén preparados los primeros dispositivos que implementan el 802.11i, los principales fabricantes, agrupados bajo la conocida Alianza Wi-Fi, se han puesto de acuerdo en este estándar provisional de seguridad.

WPA[10] se basa en un subconjunto de aspectos que se han extraído del futuro estándar 802.11i incluyendo las siguientes tecnologías para atender las vulnerabilidades WEP:

- 802.1X. Estándar creado por la IEEE en el 2001 para proporcionar un control de acceso en redes cableadas basado en el uso de puertos. Las estaciones tratarán de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentique.
- EAP. Protocolo de Autenticación Extendido (Extensible Authentication Protocol), definido en la RFC[11] 2284. Lleva a cabo las tareas de autenticación, autorización y contabilidad. EAP fue diseñado originalmente para el Protocolo Punto a Punto (PPP - Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y un servidor RADIUS. Esta forma de encapsulamiento de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP Over LAN).
- TKIP. Protocolo de Integridad de Llave Temporal (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de una llave para cada trama.
- MIC. Código de Integridad de los Mensajes (Message Integrity Code). Código que verifica la integridad de los mensajes. También conocido como Michael.

En teoría WPA puede operar simultáneamente con equipos basados todavía en 802.11 y WEP, aunque con la desventaja de que las claves de cifrado no son dinámicas. Esta limitación es muy importante ya que reduce su funcionalidad casi al mismo nivel que WEP, aunque la integridad obtenida con Michael es una ventaja. La Alianza Wi-Fi no recomienda este modo de trabajo mixto debido a que casi invalida las ventajas de WPA y en sus pruebas de certificación verifica que, si es soportado, no sea el modo por defecto.

Las experiencias de los usuarios indican que es difícil conseguir esta interoperabilidad entre productos de diferentes marcas e incluso entre los de la misma casa.

Otra limitación de WPA es que no da soporte a redes inalámbricas, cuya topología es, ad-hoc.

---

[10] Wi-Fi Alliance. "Wi-Fi Protected Access- Overview". URL: http://www.wi-fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

[11] RFC - Solicitud de Observaciones (Request for Comments). Metodología utilizada para conformar un estándar. Cada RFC detalla el funcionamiento de cada modulo incluido en un estándar.

## II.4. C. I) MODOS DE FUNCIONAMIENTO DE WPA

WPA puede funcionar en dos modos:

1) Con servidor AAA[12], RADIUS o IAS normalmente. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autenticación, autorización y contabilidad.

2) Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes, denominadas SoHo (Small Office Home Office). 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 autenticación, pero no para el cifrado de los datos.

## II.4.C. II) WPA: 802.1X Y EAP

WPA adopta al 802.1X para atender el problema de la autenticación y escalabilidad de usuarios en WEP. 802.1X inicialmente esta diseñado para redes cableadas pero es también aplicable a redes inalámbricas. El protocolo de autenticación extensible (EAP - Extensible Authentication Protocol) es un protocolo de seguridad de capa 2, del modelo OSI, empleado en la etapa de autenticación del proceso de seguridad, con lo cual se provee la capa final de seguridad para las redes inalámbricas. El estándar provee control de acceso basado en puertos así como autenticación mutua entre clientes y puntos de acceso usando un servidor de autenticación.

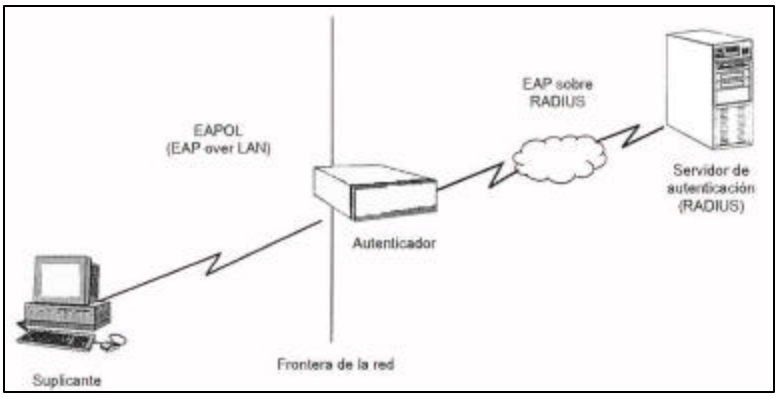



FIGURA II - 7. ARQUITECTURA DE UN SISTEMA DE AUTENTICACIÓN 802.1X

El estándar 802.1X[13] consta de tres elementos como se observa en la Figura II-7:

- Un suplicante - Un dispositivo inalámbrico que desea conectarse a la red y ser autenticado.
- Un servidor de autenticación - Un sistema de autenticación, tal como un servidor RADIUS o IAS, el cual maneja las autenticaciones. 802.1x fue diseñado para emplear servidores RADIUS (Consulte Glosario), cuya especificación se puede consultar en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.
- Un autenticador - Es un dispositivo que actúa como un intermediario entre un suplicante y un servidor de autenticación. Usualmente, es un punto de acceso.

[12] AAA - De sus siglas en inglés: Authorization, Authentication and Accounting. Se refiere a un servidor que provee las tareas de autenticación, autorización y contabilidad.
[13] Snyder, Joel. "Whast is 802.1X?" May 06, 2002. URL: http://www.nwfusion.com/research/2002/0506whatisit.html

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servicio RADIUS. Esta autenticación mutua en 802.1X involucra varios pasos como se muestra en la Figura II-8 y se explica a continuación:

1. Un suplicante inicia una conexión con un autenticador, el cual, detecta la solicitud de inicio y habilita el puerto del suplicante. Sin embargo, todo el tráfico, incluyendo DHCP, HTTP, FTP, SMTP y POP3, es bloqueado; excepto 802.1X.
2. El autenticador requiere la identidad del suplicante.
3. El suplicante responde con su identidad al autenticador, que, pasa la identidad a un servidor de autenticación.
4. El servidor de autenticación certifica la identidad del suplicante. Una vez autenticado, un mensaje de ACEPTACION es enviado al autenticador. Éste cambia el puerto del suplicante a un estatus de autorizado.
5. El suplicante solicita la identidad del servidor de autenticación. El servidor de autenticación pasa su identidad al suplicante.
6. Una vez que el suplicante autentica la identidad de un servidor de autenticación, todo el tráfico es permitido.

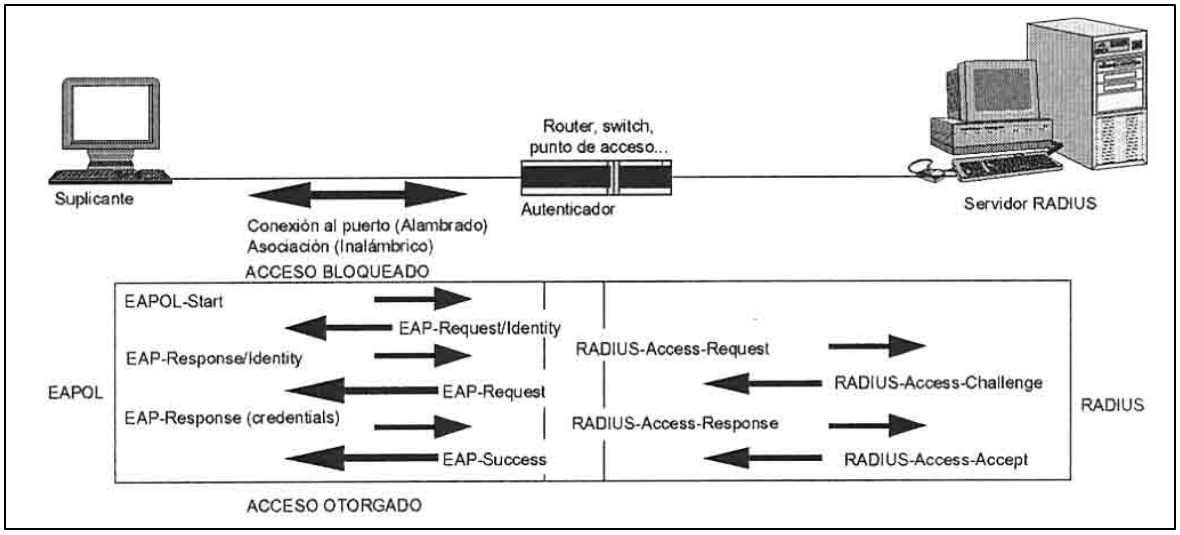



FIGURA II-8. DIÁLOGO DETALLADO: SUPLICANTE - AUTENTICADOR - SERVIDOR RADIUS

## MÉTODOS EAP

El Protocolo de Autenticación Extendido (EAP - Extensible Authentication Protocol) es el protocolo que 802.1X usa para administrar la autenticación mutua. El protocolo provee una base generalizada para un sistema de red inalámbrico al escoger un método específico de autenticación para autenticar. El método de autenticación puede ser password, certificados PKI u otras formas de autenticación.

Con EAP, un autenticador no necesita entender los detalles sobre los métodos de autenticación. El autenticador simplemente actúa como un interceptor de paquetes EAP a ser enviados de un suplicante a un servidor de autenticación, en el cual la autenticación en si se lleva a cabo.

Existen diversas variantes del protocolo EAP[14], 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: Este es un estándar desarrollado por la compañía Microsoft y definido en el RFC 2716, utiliza un certificado X.509 para realizar la autenticación, en lugar de la combinación usuario/password. Requiere de instalar 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. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate).
- 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, agilizando el proceso. Esto garantiza la autenticación 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, con lo cual el suplicante se identifica con una combinación nombre / contraseña.
- PEAP: Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAPTTLS, 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.

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).

[14] IEC. *EAP Methods for 802.11*. *"Wireless LAN Security"*. URL: http://www.iec.org/online/tutorials/acrobat/eap_methods.pdf

- 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 (smart card), lo que obligaría a instalar hardware adicional en las terminales para leer dichas tarjetas.

Las variantes de EAP que utilizan 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 la compañía 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.

- EAP-SPEKE: Esta variante emplea el método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite verificar que tanto cliente como servidor comparten una información secreta (en este caso, una contraseña) a través de un medio inseguro. Se ha comprobado que el método es muy seguro, aun con contraseñas cortas. Ofrece protección contra ataques de diccionario, así como el servicio de autenticación mutua sin necesidad de certificados. Muchos proveedores lo implementan por ser un método de autenticación robusto y sencillo.

Otra ventaja de este tipo de claves para entornos domésticos es que puede constar de cualquier tipo de caracteres (frases de entre 8 y 63 letras, incluyendo espacios) por lo que es más fácil de recordar y utilizar. La sencillez de uso que proporciona hará que muchos usuarios de pequeños entornos de red la usen y esto *"per se"* ya es un adelanto. Es un hecho que un alto porcentaje de usuarios de redes inalámbricas dejan la configuración de sus equipos tal y como viene de fábrica, sin sacar partido siquiera a las características de WEP que, por otra parte, para ellos serían más que suficientes. El hecho de que la clave PSK sea tan sencilla de establecer posibilita que mucha más gente la use.

## II.4.C. III) WPA: TKIP

Protocolo de Integridad de Llave Temporal, TKIP (Temporal Key Integrity Protocol) es otro elemento derivado del 802.11i[15]. Esta diseñado para corregir las vulnerabilidades conocidas de WEP en el área de *encriptación de datos*. Específicamente, TKIP repara la falla de seguridad del uso cíclico de llaves en WEP.

El paquete de TKIP esta compuesto de tres partes:

1) Una llave dinámica y temporal, incrementada de 40 bits en WEP a 128 bits en TKIP, la cual es compartida por los clientes y los puntos de acceso.
2) Una dirección MAC de un dispositivo cliente.
3) Un vector de inicialización de 48 bits describe un número de secuencia de paquetes.

Esta combinación garantiza que varios clientes usen diferentes llaves.

Para ser compatible con hardware existente, TKIP usa el mismo algoritmo de encriptación (RC4) usado en WEP. De tal manera, que solamente una actualización en software o firmware es requerida para implementar TKIP. Comparado con WEP, TKIP cambia las llaves temporales cada 10,000 paquetes. Esta distribución dinámica deja a los hackers un pequeño espacio para romper la llave TKIP.

En general, muchos expertos de seguridad creen, erróneamente, que TKIP tiene una encriptación mayor que WEP. Sin embargo, están de acuerdo que TKIP debe ser una solución temporal debido al uso del algoritmo RC4.

## II.4.C. IV) WPA: MICHAEL

Es usado para asegurar la integridad de los datos. El código de integridad mensajes (MIC) es un mensaje de 64 bits calculado usando el algoritmo "Michael"[16]. Su finalidad es detectar posibles cambios en el contenido del paquete debido a errores de transmisión o manipulación intencional.

## II.4. C. V) WPA-PSK

Existe un caso especial en la implementación de 802.1X. En ambientes de usuario pequeños tal como en hogares o pequeños negocios, un servidor de autenticación puede no ser una opción para autenticar. Por lo cual, un mecanismo de llave compartida con antelación (PSK - *Pre-Shared Key*) es usado. La llave compartida es puesta tanto en el suplicante como en el autenticador manualmente. Una autenticación similar a WEP es realizada.

Como su propia denominación nos indica, su único requerimiento es compartir una clave entre los diferentes clientes que se van a autenticar contra un determinado punto de acceso que también la conoce. Si la clave de un cliente inalámbrico coincide con la del correspondiente AP se le otorga

[15] Geier, Jim. "802.11 Security Beyond WEP". June 26, 2002. URL: http://www.80211-planet.com/tutorials/article.php/1377171
[16] Johnson, David. "Assorted 802.11 Related Crypto Algorithms". URL: http://www.deadhat.com/wlancrypto

acceso, denegándolo en caso contrario. Esta clave no se envía al AP al intentar la autenticación sino que es el origen de un trabajo criptográfico que finalmente conduce a la autenticación, por lo que no es posible averiguarla rastreando las emisiones. Está claro que no es tan seguro como el uso de un servidor RADIUS pero será más que suficiente en entornos que necesitan conectar de forma segura a pocos equipos.

## II.4.C. VI) CÓMO ACTUALIZARSE A WPA

WPA requiere la actualización de todos los componentes que intervienen en una red inalámbrica:

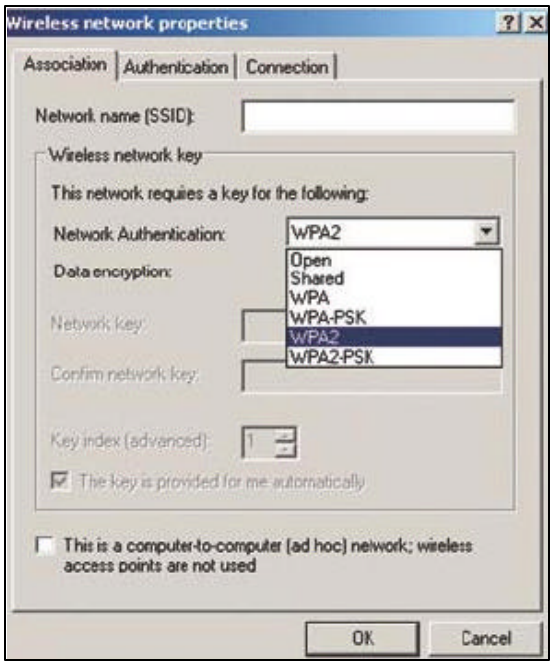



FIGURA II - 9. ACTUALIZACIÓN A WPA BAJO WINDOWS

- Firmware[17] de puntos de acceso y tarjetas de red.
- Los controladores de dispositivo.
- Software instalado en los equipos cliente.

Hay que ser claros en esto y hay que decir que es una tarea complicada al día de hoy.

Los dispositivos de red inalámbricos (puntos de acceso y tarjetas de red), requieren una actualización del firmware. Esto es necesario para poder incorporar TKIP, Michael, AES y un elemento de información nuevo que emiten los puntos de acceso.

Los primeros productos con WPA comenzaron a salir al mercado a mediados del 2005, todavía no abundan puesto que la implementación no es trivial y lleva tiempo. Algunos modelos de Cisco, 3Com y otras empresas, ya disponen de la correspondiente descarga en sus sitios Web. Sin embargo, otra circunstancia que se está dando es que muchos fabricantes dan prioridad a sus productos más recientes, ofreciendo actualizaciones sólo para productos 802.11g y dejando de lado los Wi-Fi originales (802.11a y 802.11b). Otros ni siquiera ofrecen actualización alguna.

Por otra parte se precisan nuevos controladores de dispositivo. Si utilizamos Windows XP SP1 o Windows 2003 el controlador de la tarjeta deberá ser capaz de soportar los servicios de WPA. Microsoft manifiesta que ha trabajado con muchos fabricantes de hardware inalámbrico para que éstos incluyan la actualización del firmware dentro de la instalación del nuevo controlador para Windows XP (Vea la Figura II - 9), de forma que al instalar el controlador en este sistema operativo también se actualiza su firmware de forma automática.

El software del cliente, es el que consigue que el sistema operativo pueda sacar partido a todas las mejoras que las actualizaciones de firmware y de controlador han proporcionado. El único sistema operativo que ofrece soporte para WPA es Windows XP SP1. Se puede descargar la correspondiente actualización gratuita en:

htp:\\microsoft.com/downloads/details.aspx?FamilyId=009D8425-CE2B-47A4-ABEC-274845DC9E91

[17] Firmware - Software, que puede ser grabado tantas veces sea necesario, en el chip de configuración de un dispositivo. Esto permite actualizarlo sin necesidad de cambiar físicamente dicho dispositivo.

Ésta actualiza el software de red y añade nuevas opciones a las pestañas de configuración de nuestro dispositivo inalámbrico para poder escoger WPA o WPA-PSK como método de autenticación (Ver Figura II.6) y TKIP o AES (en los casos que esté soportado) como sistema de cifrado de datos.

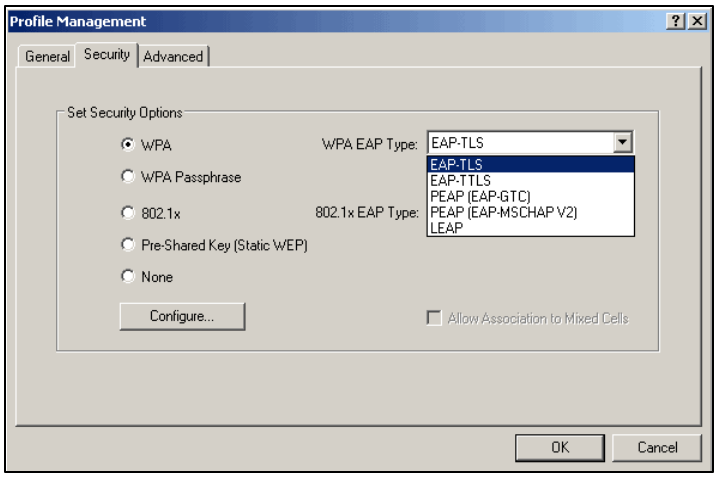



FIGURA II - 10. CLIENTE INALÁMBRICO CON OPCIONES DE SEGURIDAD.

Existen en el mercado algunos "suplicantes" de terceros que permiten utilizar WPA desde otros sistemas operativos. El más señalado en Internet es AEGIS del fabricante Meetinghouse Data Communications[18] (Vea la Figura II - 10) que funciona en Linux, MacOS X, Windows XP/NT/2000/98/Me y Pocket PC 2002, aunque cuesta unos 40 Euros. Apple dice que Mac OS X 10.3 soportará WPA sin problemas. Algunos fabricantes de adaptadores de red inalámbricos ofrecen su propio suplicante pero son los menos.

Como vemos WPA es una tecnología muy interesante que nos ayudará de una vez por todas a mantener nuestras redes inalámbricas seguras sin demasiado esfuerzo.

La triste realidad es que sin embargo será difícil poner en marcha una red de este tipo ya que la mayoría de los dispositivos no disponen de la necesaria actualización y nuestro sistema operativo no proporciona el software adecuado salvo si es Windows XP.

Si queremos sacar partido a WPA lo más probable es que debamos usar Windows XP en todos los clientes y, en muchos casos, adquirir nuevos adaptadores de red. Eso sí, a medida que se vayan renovando las redes inalámbricas en unos casos, e incorporando a la empresa en otros será cada vez más frecuente encontrar redes Wi-Fi basadas en WPA, con lo que la seguridad estará más generalizada de lo que es común hoy en día.

Para ahondar en detalles y nuevas versiones o características respecto a WPA puede consultar el sitio Web de la Alianza Wi-Fi en: http://www.Wi-Fialliance.org/OpenSection/protected_access.asp.

## II.4.C. VII) RESUMEN DE BENEFICIOS WPA

WPA soluciona la debilidad del vector de inicialización (VI) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar $2^{48}$ combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los VI, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de paquetes.

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

[18] Meetinghouse Data Communications URL: http://www.mtghouse.com/products/client/index.shtml

Las claves ahora son generadas dinámicamente y distribuidas de forma automática (TKIP) por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autenticación, se sustituye la clave compartida de WEP por la terna 802.1X / EAP / RADIUS y se tiene la posibilidad de verificar las direcciones MAC de las estaciones.

En resumen, las ventajas de seguridad de WPA sobre WEP son:

- Aplica controles más fuertes de acceso a la red usando autenticación mutua.
- Soporta las tecnologías de seguridad: 802.1X, EAP, RADIUS y llaves (PSK) pre-compartidas.
- Adopta llaves dinámicas en TKIP (48 bits) para establecer una mejor administración de llaves.
- Asegura la integridad de datos usando el nuevo algoritmo MIC.
- Provee compatibilidad futura con 802.11i.

Sin embargo, WPA también presenta algunos aspectos potenciales de seguridad:

- Existen aún debilidades de encriptación en TKIP. Afortunadamente, se espera que el rompimiento exitoso sea difícil y lento.
- El desempeño puede ser potencialmente sacrificado debido a los cálculos de autenticación más complejos e intensos y a los protocolos de encriptación.
- La fortaleza de WPA aún permanece incierta hasta probarlo contra ataques futuros. Lo que si se sabe es que es susceptible a los ataques de diccionario y de fuerza bruta.

## II.4.D) WPA2

En septiembre del 2004, la Alianza Wi-Fi liberó WPA2, el cual es una versión actualizada de WPA basada en el estándar 802.11i, es de hecho otro nombre para 802.11i. Utiliza AES-CCMP, un algoritmo de encriptación más fuerte, que el RC4 usado por WPA. Es el algoritmo de clave simétrica más seguro existente pero requiere mayor capacidad de procesamiento para implementarlo. Este es el motivo de que su uso sea opcional en WPA ya que una gran parte del hardware existente en los dispositivos inalámbricos es insuficiente para ejecutarlo. Sin embargo, algunos fabricantes, lo ofrecen en las actualizaciones de sus productos, el cual provee una encriptación suficientemente fuerte para alcanzar los requerimientos de la especificación FIPS[19] 140-2, el cual es obligatorio para muchas de las agencias del gobierno de los Estados Unidos.

WPA2 soporta TKIP, AES-CCMP, Ad-Hoc, 802.1x/EAP, PSK y modo conjunto de trabajo con WPA para facilitar la transición a WPA2. Soporta también movilidad rápida, al pre-autenticar el usuario en los puntos de acceso existentes en al infraestructura de red, permitiendo al usuario moverse sin tener que autenticarse con cada uno de ellos.

Muchos proveedores tendrán que incluir en sus dispositivos inalámbricos, hardware con la capacidad de manejar AES para no comprometer el desempeño en las WLANs. Debido a esto se deben reemplazar los equipos inalámbricos instalados. Adicionalmente se requiere de un servidor AAA como RADIUS o IAS para uso corporativo con requerimientos de seguridad altos.

[19] FIPS - Estándar que obliga el uso de AES y EAP-TLS, para procesamiento de Información de uso en agencias del gobierno federal de los Estados Unidos (US Federal Information Processing Standard)

## II.4.E) 802.11I: LA SOLUCIÓN DE SEGURIDAD DEL IEEE PARA WLANS

El nuevo estándar de seguridad, el 802.11i, para WLANs es la solución que el IEEE diseñó para resolver los problemas de WEP:

- La encriptación no estaba siendo usada apropiadamente.
- No había manera de prevenir la falsificación de mensajes.
- Las llaves de encriptación eran reutilizadas, permitiendo con esto que los datos fueran leídos sin saber la llave de encriptación.
- La autenticación no funcionaba, ya que se transmitía al aire todo lo necesario para que un atacante se autenticara ante la red.

El grupo de trabajo 802.11 "i" , conformado por expertos en seguridad, liberó esta solución en Junio del 2004. Utilizó más de tres años en la especificación y tres borradores fueron publicados durante su desarrollo.

802.11i - o oficialmente "Mejoras a MAC para una seguridad elevada"- es conocida como "WPA2" e incorpora todas las características de WPA. La cual, fue introducida al mercado por la Alianza Wi-Fi a mediados del 2003 como una medida temporal para llenar el hueco de seguridad dejado por el estándar WEP.

En la Figura II-11 se muestra un diagrama de estados de de seguridad del 802.11i.

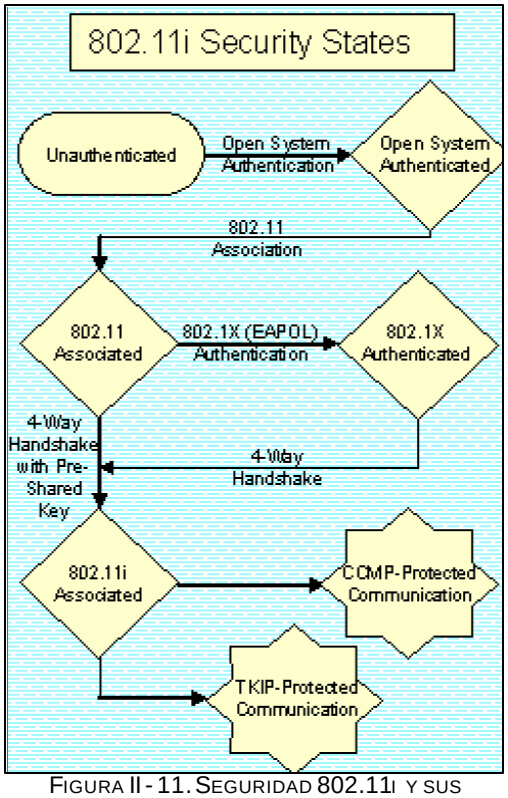



FIGURA II - 11. SEGURIDAD 802.11I Y SUS PROCESOS

Algunos de los participantes en la solución de seguridad 802.11i fueron Intel, Cisco, Agere, Broadcomm, Hi-FN, Microsoft, RSA Labs y muchos otros. Representantes de diversas Universidades como el MIT (Instituto de Tecnología de Massachusetts), Certicom y en California: Berckley y Davis. Así como la contribución de un criptógrafo independiente Danés, quién desarrollo pruebas matemáticas para delimitar la seguridad de diferentes piezas del protocolo y determinar exactamente cuanta seguridad proveían esas porciones del protocolo.

El comité "i" precedió a trabajar en cuatro líneas separadas:

1) Mejorar Autenticación. - Protocolo 802.1x, que requiere de un servidor de autenticación.
2) Inventar un nuevo algoritmo de encriptación. - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), protocolo de respuesta a la codificación en bloque encadenado al código del mensaje de autenticación y utiliza el algoritmo AES para encriptación.
3) Diseñar una solución temporal para WEP resultando en WPA: TKIP y 802.1X.
4) Asegurarse de que las llaves no fueran reutilizadas para desligar la protección de los datos de la autenticación. Ya que cada vez que un cliente se asocia con un punto de acceso se genera una llave de sesión que será usada como la base de la encriptación.

WPA proporcionó una encriptación un poco mejorada vía TKIP, rotación de llaves y un versión "cliente" con una configuración simplificada y una versión "empresarial" incorporando una variedad de combinaciones de seguridad basadas en RADIUS.

WPA2 / 802.11i básicamente añade encriptación mejorada vía AES (CCMP). Soporte a redes en modo "Ad Hoc" o IBSS y una característica llamada "pre-autenticación", la cual permite movilidad al usuario entre las redes inalámbricas conectadas en la misma infraestructura al pre-autenticar en los puntos de acceso al usuario ya autenticado en alguno de ellos.

Uno de los motivos del retraso de WPA2 fue el de dar tiempo a los fabricantes de chips para poder soportar AES en los nuevos productos. AES requiere más poder de cómputo que el débil WEP. Algunos de estos fabricantes han agregado AES en su hardware en sus conjuntos de chips, mientras que otros lo han implementado en el controlador (driver). Muchos productos inalámbricos basados en el chip Broadcom 11g han provisto AES como una opción desde la introducción de WPA y el parche WPA de Microsoft ya lo soporta.

Los usuarios pueden solo esperar que la transición de WPA a WPA2 vaya mejor que la de WEP a WPA, la cual fue larga, lenta y en muchos casos una promesa vacía para los productos existentes. Hoy en día, la mayoría de los productos 802.11b aún permanecen sin soporte WPA, forzando una actualización a productos 802.11g para aquellos usuarios que quieren mejorar la seguridad. Afortunadamente, los fabricantes tenían el incentivo de los productos 11g basados en una velocidad inalámbrica mayor como estímulo principal de actualización.

En el 2006 será obligatorio el uso del 802.11i ó WPA2. La Alianza Wi-Fi lo esta certificando los productos bajo el nombre WPA2.

La administración de estándares de China (SAC - Standards Administration of China) desarrolló su propio estándar de encriptación inalámbrica, conocido como WAPI (Wired Authentication and Privacy Infraestructure). WAPI es incompatible con el 802.11i. SAC esta intentando hacer WAPI un estándar internacional, y ha propuesto WAPI al comité JTC1 (Joint Technical Committee 1) del ISO y a la Comisión Electrotécnica Internacional (IEC - International Electrotechnical Commission).

En Noviembre del 2004, el JTC1 SC6 (Subcomité 6 - que trata los asuntos de los estándares WLAN) se reunió y presento la propuesta WAPI de SAC al IEEE 802 para su consideración de ser incorporado en las series 802.11, una moción que Intel esta alentando.

Estas especificaciones ayudan a hacer los dispositivos inalámbricos más seguros. Con 802.11i, la cadena completa de seguridad al registrarse (login), intercambiar credenciales, autenticarse y la encriptación son mucho más robustos y efectivos al brindar protección contra ambos tipos de ataques: sin objetivos fijos o con objetivos fijos.

Intel esta ahora lanzando su procesador Intel Centrino basado en tecnología móvil que incorpora la seguridad 802.11i.

Mayor información puede ser encontrada en las páginas de Web de: Intel y de la Alianza Wi-Fi.

## II.4.E. I) PROTOCOLOS UTILIZADOS EN 802.11I

El 802.11i define nuevos estándares y se basa en mucho estándares existentes.

### 802.11I UTILIZA LOS PROTOCOLOS EXISTENTES:

### 802.1X (EAPOL)

Usado para encapsular los mensajes EAP en redes inalámbricas Ethernet. De esta manera no importa cual sea el método EAP utilizado, EAPol servirá como transporte de dicho método al encapsularlo en él. Vea los diferentes métodos EAP (LEAP, TLS, PEAP, TTLS, ) en éste Capítulo en la sección II.4.C.II.

### EAP- TLS

Aunque éste no es un componente oficial del estándar 802.11i, es el protocolo de autenticación *de facto* utilizado en redes inalámbricas 802.11i. Sin embargo el uso de e EAP-TTLS a un estándar de seguridad inalámbrico podría habilitar a una WLAN para comunicarse de manera segura sin uso de certificados de encriptación.

### RADIUS

Tampoco es un componente oficial de 802.11i, pero es el estándar *de facto* para proveer autenticación. Consulte el Glosario para mayor información respecto de su funcionamiento.

Ambos componentes, RADIUS y EAP-TLS, quedan fuera de la norma como componentes oficiales del 802.11i (Vea la Figura II-12), es decir, su uso es intercambiable por algún otro.

Ya que se puede utilizar cualquier otro método EAP o RADIUS como por ejemplo EAP-LEAP e IAS respectivamente. Las debilidades que afecten éstos métodos no oficiales en el 802.11i, serán consecuentemente, puntos de debilidad para éste protocolo.

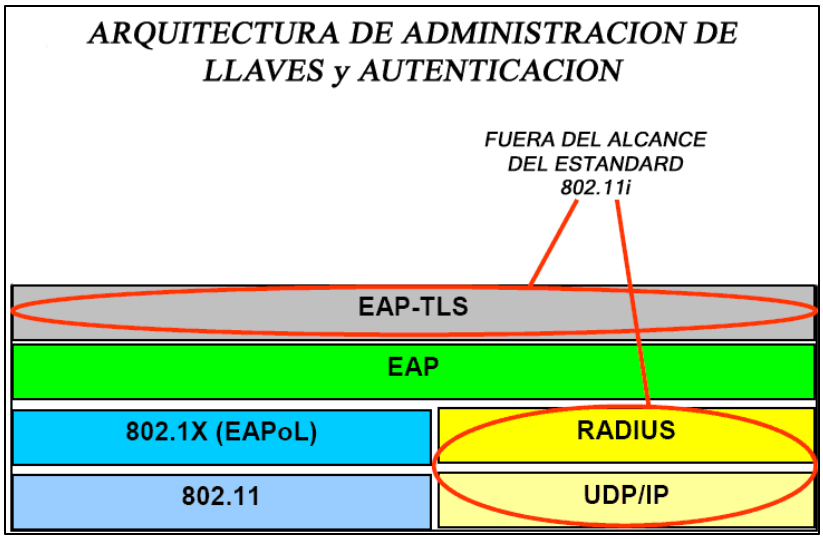



FIGURA II-12. ELEMENTOS NO OBIGATORIOS DEL 802.11I

## 802.11I DEFINE LOS PROTOCOLOS:

### WRAP Y CCMP

El Protocolo Inalámbrico de Autenticación Robusta (WRAP - Wireless Robust Authentication Protocol) es un protocolo de encriptación en el estándar 802.11i. Esta basado en el modo AES de compensación de un libro de códigos o símbolos (OCB - Offset Codebook).

Los problemas respecto a los derechos de propiedad de este protocolo, reclamados por tres diferentes grupos han causado que el IEEE introduzca el CCMP en el estándar 802.11i y hacer de WRAP un componente opcional de RSN.

CCMP utiliza una estructura de llaves jerárquicas, basadas en pares de llaves y llaves de grupo. Las fases operacionales son: Descubrimiento, Autenticación, Administración de Llaves y Transferencia de Datos.

### MIC

El verificador de integridad de mensajes (MIC - Message Integrity Check), es también parte del 802.11i y tiene una función muy similar al ICV utilizado en WEP. Sin embargo, el ICV solo protege al contenido del paquete, pero no a su encabezado. El MIC protege a ambos al paquete y al encabezado.

El MIC es un campo adicional de 8 bytes que esta entre la porción de datos de una trama 802.11 y los 4 bytes del Valor de Comprobación de Integridad (ICV - Integrity Check Value).

El algoritmo que implementa el MIC es conocido como Michael. El cual también implementa un contador de tramas, lo cual detiene ataques de repetición.

Algunos analistas se refieren a MIC como un componente de TKIP.

### RSN

RSN es un protocolo que reemplaza al TKIP y que sirve para negociar el tipo de cifrado a utilizar y así establecer comunicaciones seguras con cada dispositivo inalámbrico en la WLAN.

RSN utiliza el 802.1x para autenticar dispositivos inalámbricos a la WLAN y provee las llaves dinámicas requeridas. Todo esto con un bajo nivel de procesamiento en el autenticador, generalmente el Punto de Acceso.

RSN funciona de la siguiente manera:

1. La tarjeta inalámbrica, del cliente, envía una solicitud de sondeo (probe).
2. El punto de acceso inalámbrico envía una respuesta de sondeo con una trama de intercambio de información RSN.
3. La tarjeta de red inalámbrica solicita autenticación a través de uno de los métodos aprobados.
4. El punto de acceso provee autenticación para la tarjeta inalámbrica
5. La tarjeta de red inalámbrica envía una solicitud de asociación con una trama de intercambio de información.
6. El punto de acceso envía una respuesta de asociación.

## EL ELEMENTO DE INFORMACIÓN DE RSN

RSN comienza por establecer un canal seguro de comunicación al emitir un mensaje de Elemento de Información (EI) a través de la red inalámbrica.

El Elemento de Información (EI) transmite (broadcast) la siguiente información:

- El total de métodos de autenticación habilitados.
- El conjunto de métodos de cifrado habilitados a transmisiones dirigidas a un equipo (unicast).
- El conjunto de cifradores de transmisión múltiple (multicast).

### AUTENTICACIÓN RSN Y LOS CONJUNTOS DE ADMINISTRACIÓN DE LLAVES

Los conjuntos de administración y autenticación de llaves soportados por RSN (Vea Tabla II-2):

| CÓDIGO | SIGNIFICADO |
|---|---|
| 00:00:00:1 | Autenticación y manejo de llaves 802.1X |
| 00:00:00:2 | Sin autenticación; manejo de llaves 802.1X |

TABLA II-2. LLAVES DE ADMINISTRACIÓN Y AUTENTICACIÓN DE RSN

### CONJUNTOS DE CIFRADORES RSN

Los cifradores (Vea Tabla II-3) soportados por RSN incluyen:

| CÓDIGO | SIGNIFICADO |
|---|---|
| 00:00:00:1 | WEP |
| 00:00:00:2 | TKIP |
| 00:00:00:3 | WRAP |
| 00:00:00:4 | CCMP |
| 00:00:00:5 | WEP-104 |

TABLA II-3. CIFRADORES SOPORTADOS POR RSN

### RSN EN LOS PRIMEROS EQUIPOS INALÁMBRICOS

Las redes inalámbricas que emplean RSN pero permiten el uso de TKIP son, algunas veces, denominadas Redes de Transición de Seguridad (TSN - Transition Security Network).
TSN es necesario debido a los equipos inalámbricos viejos que no tienen el hardware suficiente para soportar el protocolo CCMP.

## II.4.E. II) RESUMEN DE BENEFICIOS Y PROBLEMÁTICAS DE 802.11I

- Canal encriptado y seguro antes de iniciar autenticación a nivel capa 2 del modelo OSI.
- Asociación y autenticación segura.
- Des-asociación y des-autenticación seguras.
- Negociación de Cifrado - Para adaptarse a los diferentes modos de cifrado en la misma WLAN, el 802.11i requiere que los dispositivos anuncien sus capacidades de encriptación, activando el tipo de cifrado apropiado basado en las capacidades mutuas de los equipos.

También se pueden aplicar políticas de seguridad que pueden ser establecidas para la red inalámbrica tal como: Solo acepta estaciones capaces de cifrar AES, etc.

- Nuevo algoritmo de verificación de mensajes: MIC.
- Metodología EAP para autenticar: EAP-TLS o cualquier otra.
- Soporte de movilidad (Roaming) al pre-autenticar en los puntos de acceso al usuario.
- Encriptación reforzada con la implementación de encriptación AES-CCMP.
- Es compatible con redes Ad-hoc (IBSS).

Los problemas del 802.11i son:

- Requerimientos adicionales de hardware, para poder implementar AES.
- Para tener una WLAN que cumpla con el estándar 802.11i en su totalidad, se requiere cambiar todos los equipos inalámbricos de la(s) red(es) instaladas.
- Debilidad ante ataques DoS y no obliga al uso específico de un método EAP.
- Una vez que se ha terminado la versión final de éste estándar tendremos que esperar tanto a la mercadotecnia, implementación y costos.

## II.4.F) RESUMEN DE LAS NORMAS DE SEGURIDAD PARA WLANS

En la Tabla II - 4 se tiene un comparativo de las diferentes normas de seguridad que han sido desarrolladas a la fecha tanto por la Alianza Wi-Fi y el IEEE.

| NORMA / CARACTERÍSTICAS | WEP | WPA | 802.11i (RSN, WPA2) |
|---|---|---|---|
| Fecha | 1999 | 2004 - Abril | 2004 - Junio |
| Algoritmo de Cifrado | RC4 | RC4 (TKIP) | Rijndael (AES-CCMP) |
| Llave de Encriptación | 40-bits | 128-bits (TKIP) | 128-bits (CCMP) |
| Vector de Inicialización | 24-bits | 48-bits (TKIP) | 48-bits (CCMP) |
| Llave de Autenticación | Ninguna | 64-bits (TKIP) | 128-bits (CCMP) |
| Integridad de los Datos | CRC-32 | Michael (TKIP) | CCM |
| Integridad del Encabezado | No | Michael | CCM |
| Distribución de Llaves | Manual | 802.1x (EAP) | 802.1x (EAP) |
| Llave única para: | Red | Paquete, Sesión, Usuario | Paquete, Sesión, Usuario |
| Llave Jerárquica | No | Proviene de 802.1x | Proviene de 802.1x |
| Negociación Cifrada | No | Si | Si |
| Seguridad Ad-Hoc | No | No | Si (IBSS) |
| Pre-Autenticación (Red Cableada) | No | No | Utiliza 802.1x (EAPOL) |

TABLA II - 4. CUADRO COMPARATIVO DE LAS NORMAS DE SEGURIDAD INALÁMBRICA.

# CAPITULO III

# REDES INALÁMBRICAS SIN SEGURIDAD: SU SIMBOLOGÍA, DETECCIÓN Y PROBLEMÁTICA

# III.1) IDENTIFICACIÓN DE REDES INALAMBRICAS VULNERABLES

## III.1.A) UN NUEVO LEGUAJE EN REDES INALÁMBRICAS

En la película WarGames (Juegos de Guerra), un joven hacker ejecuta una intrusión a una red usando un modem, lo cual acuño la frase WarDialing.

En Londres, Ben Hammersley y su amigo, Matt Jones -quien había puesto unos símbolos en un sitio Web[1] con la intención de crear un conjunto de símbolos internacionales que hicieran saber a la gente que una conexión inalámbrica estaba disponible- fueron los creadores del fenómeno llamado WarChalk (Guerra con dibujos de gis).

Ben tomó un pedazo de gis y dibujo varios de esos símbolos frente a la cafetería donde el había instalado un punto de acceso, ya que lo quería compartir con la gente. Fue así que se convirtió en el primer WarChalker (Ver Figura III-1).

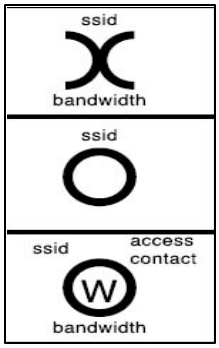



FIGURA III-1. SIMBOLOS DE WARCHALK

Poco después de que Matt publicó esos símbolos en Internet la voz se propago rápidamente y esos dos individuos iniciaron un fenómeno en Internet resultando nuevas palabras con nombres tales como *WarChalking, WarSpying, WarSpamming y WarDriving* - todo esencialmente independiente a la evolución del acceso inalámbrico.

Para aclarar, ninguno de estos nuevos términos mejoran la seguridad de la red inalámbrica. Son simplemente términos que los atacantes usan para describir sus actividades.

## III.1.B) DETECTANDO REDES INALÁMBRICAS VULNERABLES

Para detectar una red inalámbrica, se utiliza una WNIC (tarjeta de red inalámbrica) conjuntamente con un software que permita verificar la existencia de puntos de acceso. En el Anexo F, se listan de algunas herramientas disponibles para lograr este cometido.

FIGURA III-2. ENVASE DE PAPAS CONVERTIDA EN ANTENA YAGI

La antena promedio de una tarjeta de red inalámbrica no es suficientemente sensitiva para localizar señales de baja a mediana potencia, para esto se usa una tarjeta de red inalámbrica del tipo USB combinada con un diseño de antena direccional Yagi[2] hecha en casa y cableada a la tarjeta USB, como se muestra en la Figura III-2.

Existen otras antenas inalámbricas más potentes que permitan detectar y encontrar señales inalámbricas. Por ejemplo, si se quiere conectar a una red 802.11b/2.4Ghz, se opta por una antena de diseño “helix” o “helical”, la cual es básicamente un diseño tubular con una serie de

[1] Matt Jones. “matt jones | Internet product design”. URL: http://www.blackbeltjones.com/

[2] Rob Flickenger. “Wi-Fi Pringles Can Yagi Antenna”. Julio 5, 2001. URL: http://3nw.com/pda/wireless/wi_fi_pringles_can_yagi_antenna.htm

cables de cobre al alrededor del centro. Este estilo de antena a la medida puede ser difícil de construir debido a sus estándares exactos y los precios de los componentes.

Las antenas estilo "exploradora de onda" pueden estar hechas de componentes baratos tales como envases de papas, envases de café o envases de jugos. Diferentes diseños dan mejores o peores resultados dependiendo del tipo de señal del tráfico inalámbrico que se esta tratando de interceptar.

Quizás no requieran aplicaciones especiales, solo una computadora portátil con Windows XP. Desde una perspectiva de seguridad, Windows XP detecta las emisiones inalámbricas y es demasiado amigable ya que fácilmente toma cualquier emisión SSID. Automáticamente trata de unirse a cualquier red inalámbrica disponible. ¿Con tal sistema operativo tan amigable, quien necesita de herramientas especiales?

Los puntos de acceso (AP) habitualmente ofrecen una configuración por defecto insegura, en la que están predefinidos -por los fabricantes- los parámetros: SSID, canal de transmisión y administración vía WEB. Generalmente no se suele habilitar ningún método de seguridad, se usan SSID fijos y conocidos (Ver Tabla III.1). Facilitando con esto el trabajo a aquellos que desean accesar de manera ilegal a las redes inalámbricas e incrementando la problemática para los encargados de la seguridad en las redes.
Si se hace con los propósitos de robar información, acceso a Internet y/o espiar redes privadas, hay que decirlo: es *ilegal*.

| COMPAÑÍA | SSID POR DEFECTO |
|---|---|
| 3Com | 101, comcomcom |
| Addtron | WLAN |
| Cisco | Tsunami, WaveLAN Network |
| Compaq | Compaq |
| Dlink | WLAN |
| Intel | 101, 195, xlan, Intel |
| Linksys | Linksys, wireless |
| Lucent/Cabletron | Roam About |
| NetGear | Wireless |
| SMC | WLAN |
| Symbol | 101 |
| Teletronics | Any |
| Zcomax | Any, mello, Test |
| Zyxel | Wireless |
| Others | Wireless |

TABLA III-1. LISTADO DE LOS SSID MÁS CONOCIDOS.

Para ejemplificar la detección de una red inalámbrica tomemos el siguiente símil:

Imagine que se encuentra en la calle con un radio AM/FM sintonizado en la frecuencia 99.5 Mhz del FM. La antena de su radio no detecta ninguna señal y por lo tanto no se escucha nada. Sin cambiar de estación ó sintonía ¿que pasaría si al dar unos pasos descubre que puede escuchar algo?. Su radio esta sintonizada en la misma frecuencia que la emisora esta transmitiendo y al entrar en el área de cobertura, ***ahora*** es capaz de escuchar dicha transmisión en su radio.

Por lo general nosotros cambiamos de estación al cambiar la sintonía o frecuencia en la que nuestro radio recibe la señal. Pero en este caso, no cambiamos de frecuencia o sintonía, simplemente caminamos por ahí y encontramos una estación que esta transmitiendo en la frecuencia que nosotros tenemos sintonizada.

Así pues, sucede lo mismo en nuestro caso de estudio cuando se trata de descubrir una red inalámbrica. Tanto el emisor como el receptor están sintonizados en la misma frecuencia. Todo lo que hay que hacer es estar en al área de cobertura del transmisor (entre los 80 a 150 mts.) para que los equipos puedan escucharse entre si.

## III.2) WARCHALKING

Esta practica se refiere básicamente a poner marcas, con gis, en el exterior de los edificios de tal manera que se puede saber de manera muy fácil que ahí existe una red inalámbrica, así como su configuración. El lenguaje como tal es realmente simple como se aprecia en la Figura III-3:


FIGURA III-3. EJEMPLO DE WARCHALK

Así como los piratas marcaban en sus mapas donde enterraban sus tesoros y los indigentes de la gran depresión de los Estados Unidos dibujaron diferentes símbolos en los edificios para indicar cosas en particular, así Bet y Matt se inspiraron.

La intención de los Warchalkers es la de publicar donde se puede obtener una conexión inalámbrica gratis, ya sea de una corporación o de una red privada inalámbrica.

Los símbolos generalmente indican cuando punto de acceso se considera “abierto” o “cerrado”, dibujando dos medios círculos contrapuestos o un circulo normal, respectivamente y que clase de seguridad tiene ese punto de acceso.

En la Figura III-3 se muestran varios ejemplos: 1) Red abierta, SSID “WLAN”, y con una velocidad de 1.5 Mbps. 2) Red cerrada con SSID “WLAN”. 3) En la parte inferior, una red cerrada o cifrada con WEP cuya clave es: AMBAR54X, SSID “WLAN” y también con una velocidad de 1.5 Mbps.

En la práctica esta metodología ha cambiado significativamente para reflejar las realidades de lo que la gente esta tratando de conseguir. Muy poca gente camina dibujando marcas en los edificios; sin embargo, la gente esta haciendo (“Chalking”) mapas usando GPSs (equipos son sistema de posicionamiento global) para mostrar exactamente donde se localizan redes inalámbricas. Búsquedas en Internet revelan esos mapas[3] en diferentes páginas Web en línea.

Uno de los beneficios añadidos de poner los mapas en línea es que no son borrados cuando llueve.

Y es de esta manera que quien así lo desee utiliza esos datos y entra a una de esas redes. Si se hace con los propósitos de robar el acceso a Internet y/o espiar redes privadas, hay que decirlo: es ***ilegal.***

### III.2.A) WAPCHALKING

Es una variante de WarChalking creada por la Comunidad para Compartir Puntos de Acceso Inalámbricos (Wireless Access Point Sharing Community), un grupo informal con un código de conducta que prohíbe el uso de puntos de acceso inalámbricos sin permiso.

El grupo usa las marcas de WarChalking como una invitación a los usuarios inalámbricos para unirse a su red inalámbrica. En términos de WapChalking, las dos medias lunas que marcan un nodo abierto, significa que un dispositivo de acceso inalámbrico esta con la configuración de fábrica, para así, ser fácilmente detectada.

[3] NetStumbler. “NetStumbler.com”. 2001. URL: http://www.wi-fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

## III.3) WARDRIVING

WarDriving hace la localización de redes inalámbricas abiertas una labor simple e incrementa el área de búsqueda exponencialmente. Hacer WarDriving es simple: se conduce por los alrededores buscando redes inalámbricas. Parte del atractivo es el uso de sistemas de GPS conectados a una computadora portátil. Esto hace WarDriving preciso y potencialmente gratificante para aquellos que buscan una red inalámbrica ya que cubren un área mayor en un vehículo (motocicleta o automóvil).

Es inquietante que casi cualquiera pueda encontrar una red inalámbrica tan fácilmente, o ¿no? Los fabricantes activan todo por defecto, sin tener en cuenta la seguridad de la red inalámbrica; esto lo hace más fácil para los WarDrivers.

Wardriving fue inventado por un hombre llamado Peter Shipley, quien tuvo la visión de tomar Warchalking al siguiente nivel:

> "Más recientemente invente "Wardriving", aunque yo no soy el primero en salir y buscar redes inalámbricas abiertas. Si fui el primero en automatizarlo con software especializado y un GPS. Cuando inicié este proyecto el uso de WEP era del 15%, después de hacer públicas mis hallazgos, un año más tarde el uso de WEP era del 33%. Es bueno saber que la gente está entendiendo el mensaje. "

Dependiendo del marco de referencia podría preguntarse si WarDriving es un crimen. Por supuesto, aquellos que lo realizan no lo ven así; sin embargo, aquellos que tienen una red inalámbrica podrían tener un percepción diferente. Mientras realizaba mi investigación, tropecé con una cita -supuestamente del FBI- que establece su posición como sigue:

> "Identificar la presencia de una red inalámbrica puede no ser un acto criminal, sin embargo, el crimen existe si se entra a la red, incluido el robo de servicios, intercepción de comunicaciones, mal uso de los recursos de cómputo, hasta incluir violaciones de los Estatutos Federales de Abuso y Fraude de Cómputo, como robo de secretos de comercio y otras violaciones federales".

Por lo tanto, si esta desplegando una red inalámbrica, sería apropiado contratar a alguien que intente encontrarla, así la seguridad depende del conocimiento de ése individuo y es su responsabilidad asegurarse que no viola ninguna ley.

El FBI ha reportado que se llevan a cabo concursos para ver quién puede encontrar la mayor cantidad de redes inalámbricas. Aquellos inmersos en la industria inalámbrica y con cierta predisposición a esto, mantienen éstos sitios[4] de Web[5]. Encontrará ligas a varios mapas WarChalked que muestran las ubicaciones GPS y en muchos casos, mucho más sobre redes inalámbricas abiertas a nivel mundial.

[4] WorldWide WarDrive". "The Official WorldWide WarDrive". 2002. URL: http://www.worldwidewardrive.org/

[5] WarDriving. "WarDriving.com". 2001-2004. URL: http://www.wardriving.com/

## III.4) WARFLYING

WarFlying es simplemente la búsqueda de redes inalámbricas mientras se vuela en un aeroplano. Sin embargo, debido a que no mucha gente tiene acceso a pequeños aviones y las herramientas necesarias para llevar a cabo el WarFlying, la ocurrencia de WarFlying es menor que el WarDriving. Debido a lo limitado del rango de las redes inalámbricas, el avión debe volar por debajo de los 1500 metros. WarFlying fue primero registrado en Perth, Australia.

WarFlying[6] tiene algunas limitaciones claras debido a que no se tiene la habilidad (al menos hoy) para triangular el punto de acceso, el cual podría estar a varios kilómetros de dónde fue detectado. A pesar de todo, existe un artículo de cómo el Valle de Silicón fue "WarFlown", es decir, el Valle de Silicón fue peinado (Ver Figura III-4) en busca de redes inalámbricas.

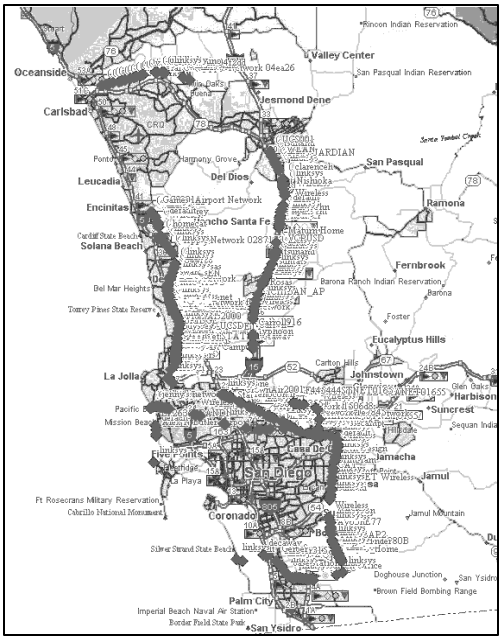



FIGURA III-4. MAPA DE WARFLYING.

## III.5) WARSPAMMING

Todos han recibido spam o correo basura; es una plaga en el correo electrónico. Creó en la libertad de expresión; sin embargo esa libertad no da el derecho a ser escuchado. Afortunadamente, los que hacen las leyes y los políticos alrededor del mundo están desarrollando leyes para penalizar a los spammers. Estas leyes pueden ser o no efectivas, el tiempo lo dirá. Sin embargo, se está volviendo más difícil para los spammers originar su spam desde países que están comenzando a desarrollar éstas leyes. Existen también organizaciones que listan, publican y bloquean las direcciones IP de lugares donde el spam se ha originado, así que, ¿que le queda al spammer por hacer?. Muchos están originando sus spam desde otros países; esto representa toda clase de problemas logísticos y costos adicionales a nuestras spammers. Como spammer, ¿que tal si pudiera manejar por ahí o contratar a alguien para encontrar una red inalámbrica abierta, unirse a esa red y enviar spam?

Sería muy sencillo encontrar una red inalámbrica abierta, unírsele y enviar spam. El atacante (spammer) podría estar sentado en la cafetería del otro lado de la calle y nunca saberlo. El spam es enviado a miles de gente que reportan lo que recibieron y aún otro problema, el spam era de naturaleza pornográfica. Pero puede ser aún peor que eso: un chequeo rápido revelará la dirección IP de la red, la cual es puesta en la lista negra y reportada a tu proveedor de servicios de Internet (ISP) y no hay que olvidar las nuevas leyes antispamming. El resultado es que todo el correo saliente de tu compañía es puesto en la lista negra. Qué pena cuando sus clientes reciben un mensaje diciendo que tu compañía está haciendo spamming, el proveedor de servicios de Internet da de baja tu conexión a Internet y los representantes de la ley tocan a la puerta. También, si la conexión a Internet se paga por uso, espere una gran cuenta este mes.

[6] Delta Farence. "War Flying : Page 1". 2002. URL: http://www.arstechnica.com/wankerdesk/3q02/warflying-1.html

La verdad en materia de WarSpamming es que su red inalámbrica lo hizo, de hecho, envió el spam a otros y mientras que pudiera haber sido el resultado de un atacante, usted es demandado porque la red inalámbrica no estaba propiamente configurada con la seguridad apropiada. ¿Quién piensa que es responsable? y ¿están ellos buscando un nuevo trabajo? Se espera ver que el WarSpamming se incremente así como se vuelve más difícil para los spammers operar. Aquellos que quieren hacer cosas cuestionables siempre encontrarán la manera; algunos se detendrán cuando se vuelva muy difícil, pero otros no.

## III.6) WARSPYING

La continuación a WarSpamming es WarSpying, el cual es un fenómeno relativamente nuevo. Este método consiste en realizar espionaje con cámaras inalámbricas o la intercepción de las transmisiones de éstas. El método más popular de WarSpying es usar cámaras inalámbricas X10. Es la cámara con mayor difusión en Internet, usada para automatizar una casa y convertirla en un casa inteligente.

WarSpying fue documentado por primera vez en la revista 2600. Esboza como hacer un dispositivo inalámbrico que pueda interceptar y adquirir el video de los sistemas de transmisión de vigilancia inalámbrica. Desde entonces, mucha gente ha explorado y documentado el tópico en línea y ahora existen reportes de gente usando toda clase de cámaras que están transmitiendo sobre una red inalámbrica. Se puede investigar más respecto de WarSpying[7], en http://www.rhizome.org/rsg/RSG-X10-1/.

Muchos lugares venden “kits” para iniciarse en WarDriving -planos, mapas y más están también disponibles. Una búsqueda simple en Internet muestra los resultados:

http://www.kenneke.com/index.html[8]

http://www.hotspotlist.com/[9]

http://www.wi-fiplanet.com/[10]

[7] Rhizome. “Rhizome Connectig Art & Technology”. 2005. URL: http://www.rhizome.org/rsg/RSG-X10-1/

[8] Kenneke Communications, LLC. “Kenneke Communications, LLC”.. 2006. URL: http://www.kenneke.com/index.html

[9] Wi-FiHotSpotList. “Wi-FiHotSpotList.com, a directory of public hot spots for finding Wi-Fi wireless Internet access network nodes”. 2006. URL: http://www.wi-fihotspotlist.com/

[10] Wi-Fi Planet. “Wi-Fi Planet - The Source for Wi-Fi Business and Technology”. 2006. URL: http://www.wi-fiplanet.com/

## III.7) ANATOMÍA DE UN ATAQUE SENCILLO A UNA RED INALÁMBRICA

A continuación se listan los pasos para ejecutar un ataque simple a una red inalámbrica.

1) Obtenga una tarjeta de red inalámbrica que acepte una antena externa. Esto permite recibir señales a distancias lejanas de sus objetivos. Este tipo de tarjetas inalámbricas pueden ser encontradas en eBay o compañías como Hyperlink Technologies.
2) Conviértase en anónimo al usar un firewall personal como el de Microsoft o como el Zone Alarm de Zone Labs, para que su computadora no sea vista ("counter-scanning") por sistemas de detección de intrusiones (IDS - Intrusion Detection Systems).
3) Use NetStumbler o algún otro scanner inalámbrico para encontrar puntos de acceso abiertos, servidores de DHCP ó direcciones IP.
4) Explote las vulnerabilidades conocidas en las redes inalámbricas. Estos métodos son las mismas que aquellas que un hacker puede usar para explotar una red cableada.
    - Use Ethereal u algún otro analizador de protocolo para husmear (sniff) las señales, obtener el tráfico inalámbrico, una dirección MAC y una dirección IP.
    - Capture la emisión de tráfico cableado (IPX, NetBIOS, ARP, OSPF, Windows y otros tipos de tráfico) para elaborar un mapa de la red.
    - De nuevo use Ethereal para ver protocolos de texto simple, tales como Telnet, POP o Http; para ver tráfico auténtico ó para capturar nombres de usuarios y passwords.
5) Use herramientas tales como SMAC para suplantar (spoof) una dirección MAC, y traspasar cualquier filtro de direcciones MAC, eliminando lo comúnmente conocido como el amarre de una dirección MAC a un usuario.
6) Use Windows para agregar la red a la lista de conexiones preferidas, o una utilería de cliente para conectarse a la RI que se tiene como objetivo.
7) Ejecute una ventana de DOS (prompt) y corra el IPCONFIG para ver si hay una IP asignada. Si no, intente IPCONFIG /renew.
8) Deambule por la red después de obtener una dirección IP.
9) Use un buscador/rastreador (scanner) de vulnerabilidades, tal como Nessus para rastrear vulnerabilidades en las estaciones de trabajo y puntos de acceso u otros dispositivos que están en la red inalámbrica.

De lo anterior, es fácil ver que no se requiere de mucha experiencia para buscar y encontrar puntos de acceso abiertos o laptops de usuarios que funcionan como puertas traseras para conectarse a la red de la corporación. Por esta razón, es importante monitorear la red por cualquier red o punto de acceso inseguro y tomar las medidas necesarias para cerrar esos puntos inseguros.

# CAPITULO IV

# BRINDANDO SEGURIDAD A REDES INALÁMBRICAS

# IV.1) LA SEGURIDAD INALÁMBRICA: UNA ACTUALIZACIÓN

## IV.1.A) LA SITUACIÓN ACTUAL

Los nuevos estándares de seguridad para redes inalámbricas (WPA2 y 802.11i) están impulsando el uso de esta tecnología en las empresas ya que la seguridad alcanzada es un asunto primordial que no se había logrado. Los primeros productos certificados WPA por la Alianza Wi-Fi fueron lanzados en septiembre de 2004. El 802.11i llegará al mercado a mediados de éste año (2006).

Según Synergy Research Group[1], las ventas mundiales totales de productos LAN inalámbricos para el hogar y la pequeña oficina en el año 2003 alcanzaron los 1.3 millones de dólares americanos, lo que representó un 60% del mercado, frente a las ventas de productos inalámbricos para las empresas que alcanzaron los 900 millones de dólares americanos. Las proyecciones al año 2007, respecto del número de usuarios, se pueden ver en la Figura IV-1.

Aunque la Alianza Wi-Fi probará productos de interoperabilidad con codificación AES, no probará, por lo menos inicialmente, la interoperabilidad entre todos los sistemas de encriptación, incluyendo muchos que son ofrecidos por diferentes proveedores. Los analistas dicen que esto puede causar problemas a las empresas que planifican la instalación de los sistemas con múltiples proveedores.

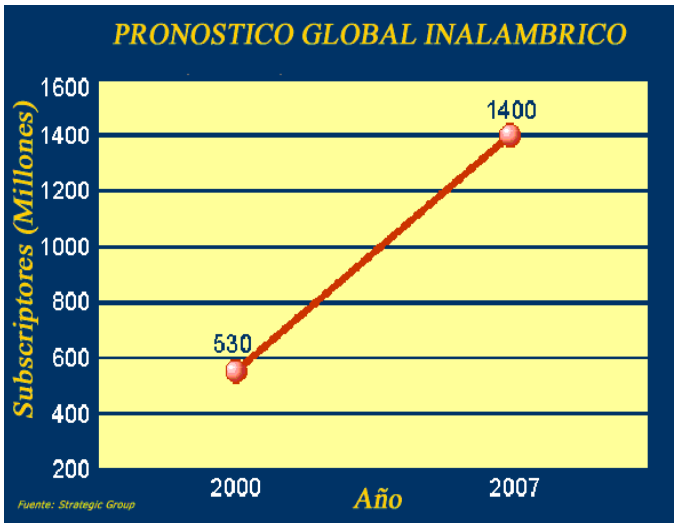



FIGURA IV-1. PROYECCIÓN DEL MERCADO INALÁMBRICO.

En la Cumbre de seguridad empresarial de Tecnologías de la Información realizada en Washington en junio del 2004, funcionarios de la firma de investigación Gartner[2] enfatizaron que las empresas deben asegurarse de que empleados y hackers no instalen AP inalámbricos no autorizados en la red inalámbrica y que los AP estén configurados de manera segura. También predicen que en el año 2006, el 70% de los ataques exitosos a las redes WLAN se producirán porque los puntos de acceso y el software de las estaciones de trabajo no cuentan con una configuración correcta.

[1] Synergy Research Group. "Synergy Research Group - SYNERGY'S HOME PAGE -". URL: http://www.srgresearch.com/store/index.asp

[2] Gartner Inc. "Gartner: Insights and advice from more than 1,000 technology experts". 2006. URL: http://www.gartner.com/Init

## IV.1.B) EVOLUCIÓN DE LAS AMENAZAS

La compañía de seguridad Symantec[3] documentó 2,636 vulnerabilidades en el 2003, 7 diarias. En el 2004 siguió un patrón similar, 80% explotadas remotamente. En el 2005, increíblemente, los ataques bajaron pero ahora se sabe que están enfocados a ciertas empresas.

Virus, gusanos, troyanos, espionaje, etc. son otros problemas y el tiempo que toma a un hacker explotar una falla es cada vez más corto, 5 días. Otra amenaza, denominada "día cero", es la que aprovecha una vulnerabilidad antes de que ésta sea anunciada y de que se publique un parche.

Internet a pasado de tener miles de usuarios en 1983 a más de 800 millones en el 2004, en el 2005 llegó a los 1000 millones, esto implica mayores riesgos (Vea Figura IV-2.).

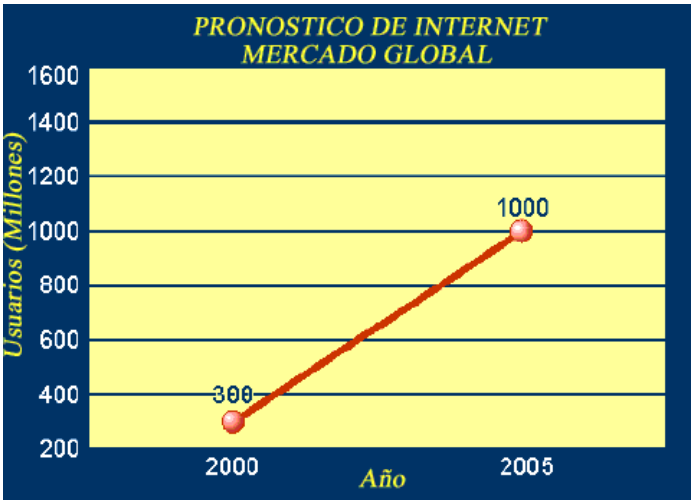



FIGURA IV - 2. MERCADO GLOBAL DE INTERNET.

Y es el comercio electrónico uno de sus grandes usuarios a razón de 24 horas al día los 7 días de la semana, revolucionando la manera de hacer negocios, pero también exponiéndonos a nuevos problemas. El crecimiento[4] de los ataques se muestra en la Figura IV-3.

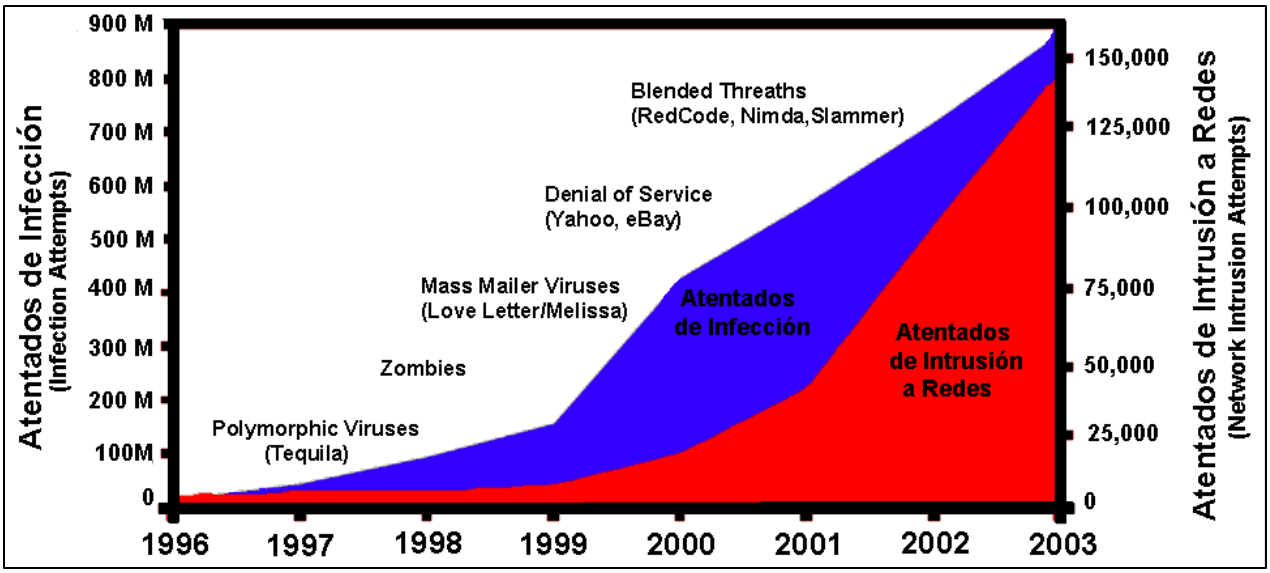



FIGURA IV - 3. TENDENCIA MUNDIAL DE ATAQUES[2].

Otro desafío significativo que afronta el personal de Tecnologías de la Información es la gran cantidad de información que necesitan asimilar para comprender y administrar la situación actual del entorno informático. Un desafío adicional es la relativa baja prioridad que el sector de software asigna a la seguridad.

---

[3] Symantec Corporation. "Symantec Corp.". 1995 - 2006. URL: http://www.symantec.com

[4] Computer Economics, Inc. "Computer Economics: Research on IT spending, budgeting, staffing, benchmark metrics and trends for the financial management of information technology". 2006. URL: http://www.computereconomics.com/

## IV.1.C) SISTEMAS DE DETECCIÓN DE INTRUSIONES

Un sistema de detección de intrusiones (IDS - Intrusión Detection System) comprueba toda la actividad hacia dentro y fuera de la red, e identifica cualquier tipo de actividad sospechosa que indicaría el ataque a la red o al sistema por un hacker que intentara penetrar en la WLAN. Los tipos básicos de IDS, como se muestran en la figura I.1, incluyen:

- Detección de pautas. El IDS analiza la información y la compara con una gran base de datos de firmas de ataques. El IDS busca una pauta de ataque específica que ya haya sido documentada. Este tipo de software de detección únicamente es tan bueno como lo sea la base de datos de firmas de ataques de hacker que se utilice al momento de comparar los paquetes. El monitoreo de IDS detecta segmentos de red cuyo estado se compara con la línea media normal y busca anomalías que se correspondan con pautas específicas de ataque.

- NIDS y HIDS. Los sistemas de detección de intrusiones basados en red (NDIS) y en servidor (HIDS) analizan paquetes individuales que viajan por la red. Los NIDS pueden detectar paquetes maliciosos que burlan las reglas de filtrado del firewall[5]. Los sistemas basados en servidor examinan la actividad de cada una de las computadoras y servidores.

- Sistemas pasivos y reactivos. Los sistemas IDS pasivos detectan una brecha potencial en la seguridad, almacenan la información, y disparan una alarma. Los sistemas IDS reactivos responden a la actividad sospechosa echando de la red a un usuario o reprogramando el cortafuego para bloquear en la red el tráfico del hacker sospechoso.

Los IDS difieren de los firewalls[1] en que éstos buscan intrusiones para que no ocurran ataques. El firewall[1] restringe el acceso entre redes para detener una intrusión; sin embargo, normalmente no puede detectar un ataque desde dentro de la red. En cambio, un IDS examina la posible intrusión una vez que ha ocurrido, y genera una alarma. Nótese que un IDS también busca ataques generados desde dentro de un sistema. Esto puede ocurrir fácilmente, ya que el usuario en una red inalámbrica aparece como “usuario interno” de la red inalámbrica , por lo tanto, es muy difícil distinguirlo de un usuario legítimo.

## IV.1.D) POLÍTICAS PARA LAS CONTRASEÑAS Y LOS SERVIDORES DE AUTENTICACIÓN

En Internet y en muchos sistemas de cómputo, las contraseñas se han convertido en la fórmula de identificación por excelencia. Gracias a ellas podemos demostrar ante un sistema quiénes somos e impedir el acceso indiscriminado de otros usuarios. Sin embargo, estamos expuestos a que un tercero pueda robar o averiguar las contraseñas y se haga pasar por nosotros.

Entre las técnicas más empleadas para averiguar contraseñas en los sistemas de autenticación se encuentran los denominados “ataques por diccionario" y "ataques por fuerza bruta”, los cuales han sido explicados en el Capítulo II. Para realizarlos con ciertas posibilidades de éxito es necesario conocer el nombre de usuario de una determinada cuenta, lo que en muchas ocasiones es muy sencillo ya que corresponde a valores por defecto (como “root”, “administrator” o “admin.”).

Muchos de los referidos ataques se dirigen a cuentas con máximos privilegios, aprovechando que el sistema utiliza un nombre de usuario conocido por defecto. Así, por ejemplo, en plataformas Windows tenemos al usuario "administrador" ("administrator" en versiones en inglés), que suele ser el objetivo más preciado. Una buena práctica de seguridad es modificar el nombre de usuario de esta cuenta por

[5] También conocido como cortafuego. Consulte el Glosario.

uno menos obvio y conocido. Adicionalmente, puede dejarse una cuenta señuelo con el nombre por defecto ("administrador"), con mínimos privilegios y una contraseña muy complicada. De esta forma, la cuenta real del administrador estará protegida y al mismo tiempo podremos detectar cualquier intento de ataque, mediante las opciones de auditoría de cuentas de usuario de Windows que permiten registrar los intentos fallidos.

### CÓMO CONSTRUIR Y UTILIZAR CONTRASEÑAS DE FORMA SEGURA

Una de las reglas fundamentales a la hora de elegir una buena contraseña se basa en su longitud y en la variedad de los caracteres que la componen, ya que cuanto mayor sea su tamaño y más heterogéneos los elementos que la integran más difícil será que la adivine un atacante. Una buena práctica consiste en crear contraseñas de al menos 8 caracteres de longitud, compuesta por letras (combinando mayúsculas y minúsculas), dígitos y símbolos especiales (un ejemplo podría ser "ke8_JW.@").

Si bien la construcción de una contraseña segura no resulta complicada, existen tantas aplicaciones y servicios que las requieren que puede llegar a ser difícil recordar todas y cada una de las empleadas en cada ocasión, y más si se tiene en cuenta que por su diseño no son series de números o palabras comunes fáciles de recordar.

Hay usuarios que optan por utilizar la misma contraseña para varias de sus aplicaciones y servicios, evitando así tener que recordar varias contraseñas diferentes. Esta forma de proceder aumenta el riesgo de que un atacante robe su identidad digital, ya que en cada una de las aplicaciones y servicios la contraseña puede ser almacenada de diferentes formas y estar más o menos expuesta ante terceros. Así, por ejemplo, si empleamos la misma contraseña para acceder al ordenador, al buzón de correo Web y a la banca electrónica, y un atacante consigue la contraseña de nuestro ordenador podrá leer nuestro correo y realizar transacciones en nuestro nombre. Por tal motivo, es conveniente utilizar diferentes contraseñas, especialmente en aquellos servicios que contienen información confidencial (como ocurre con la banca electrónica), y sólo emplear contraseñas fáciles y comunes para servicios menos comprometidos (como, por ejemplo, la cuenta para leer el periódico on-line).

Frente a los métodos tradicionales se encuentran los certificados digitales, siendo los más conocidos por los usuarios los que se hallan en los servidores Web seguros -como la banca electrónica- y permiten establecer conexiones cifradas a través del protocolo HTTPS. Los certificados digitales para clientes son similares pero, en este caso, permiten verificar la identidad del usuario, añadiendo una capa adicional de seguridad a los sistemas basados únicamente en contraseñas.

En la actualidad, ya son varias las entidades bancarias que están emitiendo certificados digitales para sus clientes. En concreto, les proporcionan un certificado que deben instalar en su PC, impidiendo así a un atacante acceder desde otro ordenador, aunque robe su contraseña de acceso. Para los usuarios móviles, que no siempre se conectan desde un PC determinado, también están distribuyéndose certificados digitales almacenados en memorias USB del tamaño de una llave convencional.

Los métodos de seguridad para redes inalámbricas combinan los certificados digitales con servidores de autenticación de nombres y claves de usuarios para poder llevar a cabo una seguridad completa, he aquí un ejemplo de las políticas de seguridad que pueden aplicarse para crear contraseñas seguras y que opciones podemos configurar en el servidor de autenticación para evitar ataques.

**POLÍTICA DE CONFIGURACIÓN DEL SERVIDOR DE AUTENTICACIÓN EN RELACION A LAS CONTRASEÑAS**

- Contraseña de 8 caracteres mínimo.
- Incluir de forma obligatoria: mayúsculas, minúsculas y símbolos.
- Cambiarlas cada 6 meses.
- Definir el Intervalo y el número de Intentos para proveer la contraseña en el servidor.
- Activar el chequeo del numero de veces que intenta el usuario su contraseña y definir cuantos intentos son permitidos. Por ejemplo: Si al tercer intento no teclea correctamente su contraseña la cuenta se desactivara por un lapso de una hora. También en el servidor.
- Solo permitir acceso desde una IP en particular.

### IV.1.E) PREVENCIÓN DE ATAQUES DE FUERZA BRUTA Y DE DICCIONARIO

Es muy difícil lograr una prevención total de este tipo de ataques. Sin embargo he aquí algunas de las metodologías más usadas para contrarrestarlos:

- Bloqueo de la cuenta del usuario ante intentos fallidos de proveer la contraseña correcta.
- Inyectar una pausa aleatoria (segundos) cuando se teclea una contraseña.
- Registrarse (login) y trabajar sólo desde una dirección IP.
- Haga uso de software para prevenir ataques automatizados. Ejemplo: Captchas.
- Monitoree las bitácoras de los servidores, en busca de un alto numero de intentos infructuosos para entrar a la red.

A continuación se dan las condiciones que pueden indicar un ataque de fuerza bruta u otros tipos de ataque:

- Intentos excesivos de entrar a la red desde la misma IP.
- Registro excesivo de entradas a la red desde la misma IP.
- Entradas a la red de una cuenta en particular de muchas IP diferentes.
- Uso excesivo del ancho de banda por un solo usuario.
- Intentos fallidos de entrada a la red usando nombres o contraseñas secuenciales.

## IV.2) DESAFÍOS IMPORTANTES DE LA SEGURIDAD DE LA INFORMACIÓN

### IV.2.A) ESCASEZ DE PERSONAL DE SEGURIDAD INFORMÁTICA

Encontrar personal cualificado en seguridad de la información es una labor difícil, y este seguirá siendo el caso en el futuro cercano. Aspectos como la inmadurez de las soluciones de los proveedores de seguridad de la información, el número limitado de personal cualificado disponible y la combinación exclusiva de habilidades requeridas para la seguridad de la información constituyen el desafío de la contratación. Los ejecutivos empresariales deberán trabajar más en esta área para superar estos retos.

Debido la inmadurez del mercado, la carencia de estándares y la gran cantidad de soluciones aisladas, la falta de entrenamiento es un problema para el personal de seguridad. El sector no ha tenido tiempo para aumentar el personal necesario para estas funciones. Además, los desafíos de la seguridad de la información siguen aumentando a gran velocidad y expanden constantemente la lista de tecnología que se debe implantar, para lo que el personal de seguridad de la información no está

preparado. Esto se traduce en más tiempo y dinero para entrenar al personal en los productos comercialmente disponibles.

Para obtener las credenciales necesarias para la seguridad de la información se requiere un entrenamiento y experiencia considerables. La credencial CISSP (Certified Information Systems Security Professionals) es una certificación acreditada internacionalmente que requiere la aprobación de un examen sobre gran variedad de temas de seguridad de la información y tener una experiencia laboral mínima de cuatro años. La credencial relacionada SSCP (System Security Certified Practitioner) exige un año de experiencia además de la aprobación de un examen.

La certificación CISM (Certified Information Security Manager) también requiere un número mínimo de años de experiencia en seguridad de la información, además de haber aprobado satisfactoriamente un examen escrito. Todas estas certificaciones exigen entrenamiento continuo como parte de la certificación y las certificaciones GIAC (Global Information Assurance Certifications) exigen una evaluación periódica cada dos años. Los profesionales de la seguridad que disponen de estas certificaciones tienen gran demanda y los empresarios deben competir para contratarlos. La certificación CISA (Certified Information Systems Auditor) requiere un mínimo cinco años de experiencia laboral antes de poder presentarse a un examen. Las certificaciones GIAC del Instituto SANS (Systems Administration, Networking and Security) requieren que los candidatos presenten un trabajo práctico como parte de la certificación. La certificación CISM (Certified Information Security Manager) también requiere un número mínimo de años de experiencia.

Además de la capacitación técnica específica, el personal de seguridad de la información debe desarrollar habilidades para el cumplimiento de la seguridad que no forman parte de la formación profesional tradicional del personal de TI. Los sectores del ejército, inteligencia y cumplimiento de la ley han realizado tradicionalmente entrenamiento en esta área. En muchos sentidos, las políticas de seguridad de una compañía son similares a las “leyes” que se deben implementar en una compañía, lo que requiere entrenamiento especializado. Este requisito único dificulta la transición del personal existente de TI para que asuma funciones de seguridad de la información sin recibir entrenamiento especializado.

Probablemente, el mayor desafío en esta área es encontrar un líder que tenga amplia experiencia en el tema y que pueda conformar un equipo eficaz de seguridad de la información. Pocos candidatos han estado en el área de seguridad de la información más de dos años y poseen la combinación requerida de habilidades técnicas y en el cumplimiento de la seguridad. También afrontan el desafío de liderazgo para contratar personal inexperto y convertirlos en profesionales eficaces en seguridad de la información, y responder a los crecientes riesgos de seguridad. Este personal es escaso y tiene gran demanda.

Los ejecutivos deberán considerar estrategias a largo plazo para satisfacer estas necesidades porque buscar personal entrenado no es solamente una cuestión de dinero, sino también de tiempo para conformar un equipo con un número limitado de personal cualificado.

## IV.2.B) LA LEGISLACIÓN DE LOS GOBIERNOS EN LA PROTECCIÓN DE LA INFORMACIÓN

En mayo del 2000, el acuerdo Safe Harbor[6] fue aprobado para las compañías de los Estados Unidos que están reguladas por la Comisión de Comercio Federal de los Estados Unidos (FTC) y que tienen operaciones en la Unión Europea. Este acuerdo les obliga a cumplir con la Directiva Europea para la protección de la información al adoptar los principios del acuerdo Safe Harbor.

Estos principios requieren controles para garantizar que la información personal esté protegida contra la pérdida, utilización indebida, acceso no autorizado, divulgación, etc. como una condición para obtener la certificación. Las compañías certificadas por el acuerdo Safe Harbor pueden obtener permiso para transferir la información fuera de la Unión Europea por periodos renovables de un año. Se puede decir sin temor a equivocarse que otros países adoptarán una legislación similar para proteger la privacidad de la información del consumidor de sus respectivos ciudadanos.

El acuerdo Safe Harbor es un ejemplo de cómo los Estados Unidos llegó a un acuerdo con la Unión Europea para cumplir con sus reglamentaciones. Otros países adoptarán estrategias similares para garantizar que sus sectores sean competitivos y que puedan funcionar independientemente en mercados importantes como el de la Unión Europea.

Un desafío importante es que ciertos países no dan mucha prioridad a la protección de la información personal o propiedad intelectual. Posiblemente tienen problemas más apremiantes, como los alimentos o medicamentos y quizás son incapaces o no están dispuestos a vigilar a las personas que están involucradas en actividades como el hackeo de software. Estos delincuentes operan libremente en estos países sin temor a que las autoridades jurídicas frustren sus operaciones. Estos refugios para los delincuentes del ciberespacio suponen mayores desafíos a las empresas legítimas que tienen pocos recursos jurídicos para combatir las actividades ilícitas de los hackers de software.

## IV.2.C) LA FUERZA LABORAL MÓVIL

El desafío, desde una perspectiva de seguridad, tiene dos aspectos: en primer lugar, toda la protección que se ofrece a la compañía debe ahora ser incorporada en la computadora portátil o aparato móvil. En segundo lugar, los protocolos 802.11 tienen funcionalidades de seguridad débiles. Cuando los empleados están en la oficina, pueden aprovechar la protección de seguridad de la compañía como firewalls, software antivirus, anti-troyanos, anti-espionaje, etc. Estos productos se pueden configurar para que funcionen en un segundo plano, los empleados no se dan cuenta de que estos productos protegen continuamente sus equips de amenazas como los virus informáticos. Cuando los empleados salen de la oficina, deben tener esta misma protección en las computadoras portátiles o aparatos de mano para que puedan seguir funcionado de manera segura y protegida. Además de que los aparatos móviles no tienen herramientas para la seguridad de la información, también corren el riesgo de robo o pérdida de la propiedad intelectual valiosa, información de los clientes u otra información confidencial que puedan tener.

Las nuevas tecnologías en general se centran inicialmente en las herramientas y funcionalidades a expensas de la seguridad para que sean acogidas y adoptadas por la masa crítica. Este es el caso de la norma 802.11, puesto que los consumidores individuales han adoptado inicialmente esta tecnología y están menos preocupados de que otra persona lea sus correos electrónicos o tenga acceso a su

[6] Safe Harbor. “U.S. Department of Commerce”. 2005. URL: http://www.export.gov/safeharbor/

libreta personal de direcciones. Por el contrario, las empresas no pueden correr riesgos porque los sistemas empresariales tienen registros vitales que podrían interrumpir sus operaciones si se divulgan a otras compañías no autorizadas. Las compañías deben pensarlo muy bien antes de invertir en el nuevo campo de la tecnología inalámbrica.

La Tabla IV-1 y el Anexo F describen algunas de las herramientas de ataque a redes inalámbricas, la mayoría , disponibles gratuitamente en Internet.

| HERRAMIENTAS / CLASIFICACIÓN | HERRAMIENTAS UTILIZADAS PARA ATACAR REDES INALÁMBRICAS |
|---|---|
| SCANNERS | APScanner, Kismet, NetStumbler, Wavemon, Wellenreiter, Wi-find, Wireless Security Auditor |
| SNIFFERS | AiroPeek, AirTraf, Mognet, LinkFerret, NG Wireless Sniffer, SSID Sniff, VPNmonitor |
| EXPLOTADORES DE PROTOCOLO | Anwrap, Asleap, Hotspotter, Pong “GSTsearch”, Ittra |
| NEGACIÓN DE SERVICIO | FATAjack, Hunter_Killer, Macfld, Michael, Void11 |
| HERRAMIENTAS MULTIUSO | AirJack, BSD-Airtools, Ettercap, LSAKnopix, Knopix, THC-RUT, WarLinux |
| EXPLOTADORES DE WEP | AirSnort, WAP Attack, WEPCrack, WEPWedgie |
| SOFT APS | HostAP, CqureAP, DiskAP, Coyote Linux |
| OTHER TOOLS | Airsnarf, AP Hopper, APTools, Fake AP, WINPCAP |

TABLA IV - 1. CLASIFICACIÓN DE HERRAMIENTAS DE ATAQUE A REDES INALÁMBRICAS

## IV.2.D) INTERCONECTIVIDAD Y FABRICANTES DE CHIPS INALÁMBRICOS CERTIFICADOS

Otro de los graves problemas de las WLANs son la incompatibilidad que tienen muchos de los productos existentes en el mercado.

Los líderes en fabricación de chips inalámbricos Atheros, Broadcom o Intel están, entre otros, certificados por la Alianza Wi-Fi. Asegúrese de adquirirlos, para tener una seguridad inalámbrica sólida y rápida, ya que al usar chips de otras marcas se tendrán problemas no sólo de seguridad sino de interconectividad, desempeño y funcionamiento.

# IV.3) LAS MEJORES PRÁCTICAS DE SEGURIDAD INALÁMBRICA

## IV.3.A) PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA: ISO17799 Y BS7799

El ISO17799 y BS7799 son políticas y estándares de procedimientos de seguridad. Conocido inicialmente como un estándar Británico, precisamente desarrollado por la Institución de Estándares Británicos. El cual fue adoptado por el comité de la ISO IEC y se convirtió en el ISO IEC JTC1 - 17799:2000, publicado el 1º. de Diciembre del 2000, de ahí su nombre.

Ambos estándares ISO17799 y BS7799 comprenden una aproximación general a los aspectos más comunes de la información relativa a archivos electrónicos, de datos y de software, documentos en papel como notas escritas a mano, materiales impresos y fotografías; grabaciones de videos y audio, comunicaciones en general incluyendo conversaciones personales, telefónicas y celulares, así como mensajes correo electrónico, fax, mensajes instantáneos, de video, etc. entre muchos otros asuntos comprendidos en la definición del término "información".

Ya que la información tiene un valor y es por lo tanto un bien, necesita ser protegido al igual que cualquier otro bien, así como la infraestructura que soporta dicha información, incluyendo todas las redes, sistemas y funciones que permiten a la organización administrar y controlar sus recursos de información. BS7799 explica que puede hacerse para proteger la información de la organización.

Hoy en día, se enfrentan un amplio rango de amenazas de seguridad, desde fallas de equipo hasta errores humanos, fraude, vandalismo, robo, sabotaje, fuego, inundaciones y aún terrorismo en muchos países, de ahí que la información necesita ser protegida. El BS7799 sugiere enfocar su atención en tres puntos principales (Vea Tabla IV-2) para garantizar la seguridad de su información:

| | |
|---|---|
| **INTEGRIDAD** | Para proteger la totalidad y veracidad de la información y los métodos usados para procesarla. |
| **CONFIDENCIALIDAD** | Asegurando que la gente que ha recibido autorización la pueda accesar. |
| **DISPONIBILIDAD** | Para garantizar que los usuarios autorizados tengan acceso a tal información y todos los recursos asociados cuando sea requerido. |

TABLA IV - 2. PUNTOS PRINCIPALES DE LA SEGURIDAD DE LA INFORMACIÓN

Al identificar los riesgos y necesidades de seguridad de la información se puede realizar una evaluación de riesgo, estudiar los requerimientos legales y examinar sus propias necesidades para desarrollar o mejorar su propio programa de seguridad de la información.

El ISO - IEC 17799:2000, ofrece lineamientos e indicaciones voluntarias para la administración de la seguridad de la información, por ejemplo:

- Establecer una política de seguridad de la organización
- Infraestructura de Seguridad de la Organización
- Clasificación y control de bienes
- Seguridad del personal
- Administración de comunicaciones y operaciones
- Control de Acceso
- Desarrollo y mantenimiento de sistemas.
- Administración de la continuidad de negocios y
- Cumplimiento o conformidad

No provee material definitivo o específico sobre ningún tópico de seguridad. Provee lineamiento general respecto de la gran variedad de tópicos listados pero no va al detalle.

Es un estándar de administración y lidia con la revisión de los asuntos no técnicos relacionados a sistemas de TI instalados. Esos asuntos tienen que ver con asuntos de seguridad: física, del personal y procedimientos de administración de la seguridad en general.

Hay una amplia variedad de publicaciones de seguridad, procedimientos y lineamientos disponibles en el sitio de Web del NIST (Instituto Nacional de Seguridad y Tecnología de los Estados Unidos): http://csrc.nist.gov/publications/nistpubs/index.html.

## IV.3.B) MONITOREO PARA MITIGAR LOS RIESGOS DE LAS WLANS

De la misma manera que las compañías pueden usar cámaras de vigilancia para monitorear amenazas físicas, las empresas deben constantemente observar sus redes inalámbricas para detectar vulnerabilidades e intrusiones. Al observar las redes cableadas e inalámbricas en conjunto es la única manera para proteger apropiadamente un red de los hackers. La Figura IV-4 nos muestra el monitoreo de una red inalámbrica.

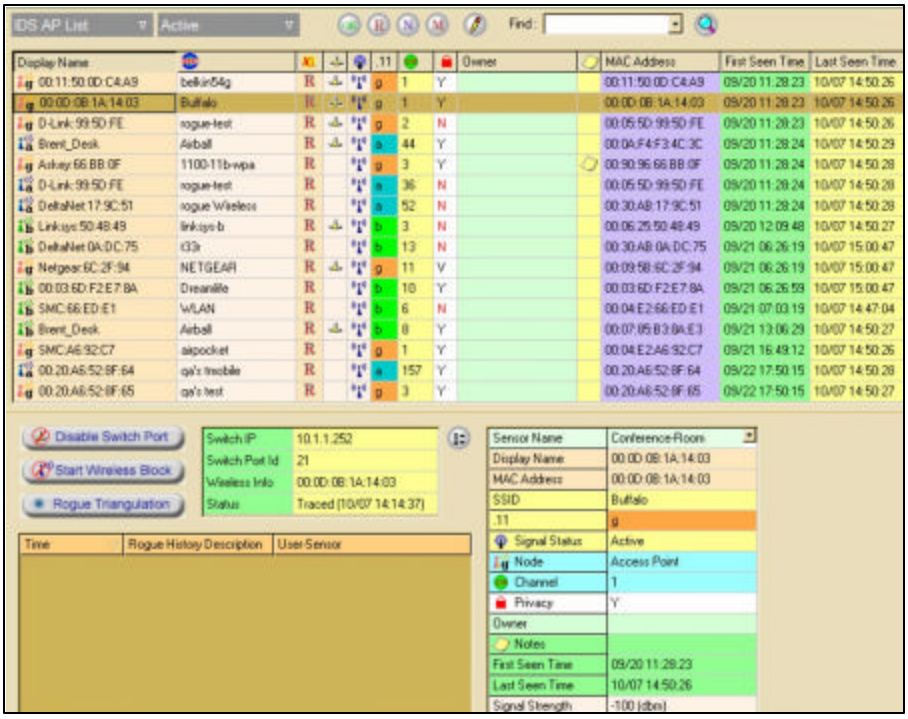



FIGURA IV-4. EJEMPLO DE MONITOREO DE RED INALÁMBRICA

Existen varios productos comerciales que proveen los siguientes servicios:

- **Análisis y Detección de puntos de acceso falsos**. Los puntos de acceso no autorizados "rogue" representan uno de las mayores amenazas para la seguridad de la red de la empresa creando un punto de entrada a la red que sobrepasa todas las medidas de seguridad existentes.
- **Protección de Intrusos**. Monitoreo en tiempo real los protocolos 802.11a/b/g para la detección más avanzada para redes inalámbricas.
- **Cumplimiento y Ejecución de Política de Seguridad**. Esto permite a las empresas crear políticas para cada dispositivo como parte de una política centralizada que define, monitorea y ejecuta las políticas.
- **Soporte operacional y Monitoreo saludable**. Monitorea la salud de la red inalámbrica y provee soporte operacional que maximiza su rendimiento y alerta cuando los dispositivos fallan o son desconectados. Provee una encuesta de la red inalámbrica para resolver problemas, hacer mejores decisiones, planear instalaciones futuras y actualizaciones.

Así como los negocios y los consumidores continúan la rápida adopción de tecnologías inalámbricas, todas las empresas deben dirigir sus crecientes inquietudes de seguridad a las nuevas amenazas aéreas. Las compañías gastan millones de dólares asegurando sus redes. Cuando una red de la compañía es expuesta por dispositivos inseguros, los hacker pueden entrar a la organización y comprometer la columna vertebral de la corporación, convirtiendo las inversiones de seguridad para tecnología de la información en obsoletas.

Las implicaciones de una seguridad rota impacta la reputación de la compañía, su propiedad intelectual y la información regulada que maneja.

## IV.3.C) DETECCIÓN DE PUNTOS DE ACCESO ROGUE

La única manera de encontrar puntos de acceso no autorizados (Rogue) es escuchar las señales.

### SNIFFERS (HUSMEADORES)

Son programas (tal como AirSnort o NetStumbler) que permiten rastrear y examinar todos los canales de radio frecuencia en busca de conexiones con cualquier punto de acceso dentro del rango.

Permiten capturar información valiosa respecto de los puntos de acceso ya que seria muy lento caminar por su compañía en busca de los no autorizados.

Más adelante, se debe determinar si un punto de acceso no conocido es ilegal (conectado a su red o no) o es simplemente ajeno (de alguna otra red pero en el rango aéreo de su red).

Mientras que este tipo de auditoria de Radio Frecuencia es valiosa, es costosa, incompleta y demasiado intermitente para continuamente proteger su red inalámbrica de puntos de acceso ilegales. Y si su red cubre un área geográfica extensa, este método de detección de rogue puede ser imposible.

### PROBES (SENSORES)

Para asegurar la continua vigilancia de Puntos de Acceso no autorizados, se pueden instalar sensores, “probes”, de tiempo completo, son dispositivos electrónicos que continuamente exploran y monitorean todo el tráfico 802.11 dentro del rango. Esto puede ser una propuesta costosa. No solo por el costo de los equipos, de entre $500 y $1000 dólares por dispositivo, pero también en términos de instalar cable Ethernet y proveer una conexión eléctrica. Es decir, costos de recursos humanos, del equipo, logísticos, etc.

Sin embargo, hay una alternativa. Si esta planeando instalar una red inalámbrica, el monitoreo dedicado no es necesario. Ya existen puntos de acceso, por ejemplo los de la compañía Orinoco, que están diseñados para actuar como sensores así como puntos de acceso, reduciendo el costo de protección contra los Punto de Acceso no autorizados(Rogue).

Consulte la sección de productos comerciales de seguridad inalámbrica al final de este Capítulo.

## IV.3.D) CONSIDERACIONES PARA UNA WLAN SEGURA - INTEL

### IV.3.D. I) IMPLEMENTE ESTÁNDARES DE SEGURIDAD ADECUADOS A SUS NECESIDADES DE NEGOCIO

Para proteger su red de problemas de seguridad, inicie por seleccionar los mecanismos apropiados de autenticación de usuarios y encriptación de datos mas apropiada a sus necesidades de negocio, presupuesto y recursos. Inicie por valorar las necesidades de seguridad para redes inalámbricas de su organización. Por ejemplo, un pequeño negocio puede no tener los recursos para instalar y manejar una solución de seguridad de nivel empresarial.

A continuación seleccione una solución de seguridad a sus necesidades de negocio. El IEEE 802.11i ratificado en Junio del 2004, utiliza un estándar avanzado de seguridad (AES), así como otras mejoras respecto de estándares de seguridad previos. La certificación de la alianza Wi-Fi para 802.11i, denominada WPA2, ha sido probada y certificada respecto a interoperabilidad. Ambas WPA2 y su predecesor, WPA, están también disponibles en versiones menores para negocios pequeños y medianos, o seguridad para redes inalámbricas caseras.

Al comprar solamente productos Wi-Fi certificados protege su inversión al proveer soluciones basadas en estándares que son interoperables entre diferentes marcas.

Para mayor información de los estándares actuales de seguridad y certificaciones, puede consultar los sitios de Web de la alianza Wi-Fi o del IEEE, http://www.wi-fi.org y http://www.ieee.org respectivamente.

### IV.3.D. II) HAGA AL USUARIO SU SOCIO EN SEGURIDAD

Los administradores de red tienen trabajo suficiente del cual ocuparse. Al emplear a los usuarios de red como agentes de seguridad, se puede ayudar a manejar riesgos futuros.

- Informe a los empleados que ellos son dueños de la seguridad y que comparten los costos de las violaciones de seguridad.
- Explique a los empleados el riesgo de instalar puntos de acceso sin el conocimiento o consentimiento del administrador de red (llamados Puntos de Acceso Rogue). Cuando los activan, frecuentemente no configuran los parámetros de seguridad adecuados, o asumen que están activados.
- Implemente un sistema donde los empleados conozcan el nombre de los puntos de acceso y enfatice la importancia de conectarse solo a Puntos de Acceso conocidos.
- Eduque a los usuarios respecto de los riesgos de seguridad al conectarse vía inalámbrica usando redes punto a punto.
- Advierta a los usuarios respecto de los peligros al conectarse en espacios públicos o compartidos utilizando redes punto a punto (ad-hoc).
- Muestre a los usuarios como verificar los mecanismos de seguridad en sus computadoras y de ser requerido como habilitarlos.

#### IV.3.D. III) IMPLEMENTE POLÍTICAS DE SEGURIDAD VIGILANTE

Sin una política que no establezca chequeos de seguridad regulares, se pone a la red en riesgo de violaciones de seguridad a futuro.

- Desarrolle una política de seguridad para redes inalámbricas y establezca objetivos a cumplir basados en esas políticas.
- Regularmente busque o rastree puntos de acceso desconocidos o no autorizados.
- Cambie las claves de administración y los SSID de los puntos de acceso.
- Implemente las últimas especificaciones de seguridad del IEEE (actualmente 802.11i).

#### IV.3.D. IV) LÍMITE EL ÁREA DE COBERTURA, LÍMITE SUS RIESGOS

Al limitar el área de cobertura de la red inalámbrica puede, de hecho, beneficiar la seguridad de su red.

- De servicio solamente a las áreas que lo requieran. Por ejemplo, los estacionamientos podrían no requerir de cobertura inalámbrica.
- Instale los puntos de acceso cerca del centro de los edificios y evite instalarlos cerca de las paredes exteriores.
- Reduzca la potencia de emisión del punto de acceso cuando y donde sea posible.
- En casos extremos se recomienda pintar o cubrir los muros con material que no permite que se difunda las señales inalámbricas.

## IV.3.E) MEJORES PRÁCTICAS DE SEGURIDAD - SYMANTEC

A la luz del actual panorama de las amenazas, Symantec cree que la mejor forma de promover un entorno laboral inalámbrico seguro es adoptando un conjunto detallado de “mejores prácticas”.

Específicamente las empresas deben:

- Establecer y reforzar la seguridad de las computadoras portátiles y crear un programa de consientización sobre seguridad.
- Garantizar la capacidad para administrar centralmente la instalación, actualizaciones y respuesta de un programa de seguridad.
- Asegurarse de que toda la configuración de seguridad se mantenga y controle centralmente.
- Implantar actualizaciones automáticas oportunamente.
- Instalar una tecnología que pueda detectar y bloquear las amenazas conocidas y desconocidas.
- Obtener advertencias sobre las amenazas con antelación para que haya una mitigación más rápida.
- Actualizar los sistemas operativos.

Hemos llegado a un punto en el que las amenazas más recientes se propagan a una velocidad mayor que la de nuestra capacidad para reaccionar ante ellas. Por otro lado, estas amenazas están causando verdaderos riesgos a las empresas como las pérdidas directas e indirectas.

Aunque el progreso en el desarrollo de la próxima generación de normas de seguridad WLAN es alentador, las empresas deben continuar tomando medidas para garantizar la eficacia de sus programas de seguridad WLAN. La protección proactiva e integral en las estaciones de trabajo y compuertas (gateways) es esencial para las compañías "sin cables".

# IV.4) CONSTRUYENDO WLANS SEGURAS

## IV.4.A) MÉTODOS BÁSICOS Y FALIBLES DE PROTECCIÓN A WLANS

A continuación veremos algunos métodos que han sido y son aún utilizados para asegurar WLANs, desafortunadamente todos ellos tienen debilidades de seguridad. Adicionalmente, sus debilidades han sido ampliamente difundidas y se han desarrollado todo tipo de herramientas de software y hardware (Vea el Anexo F) para explotarlas.

En el Capítulo II se abordaron algunos de ellos como parte de la evolución que ha tenido la seguridad en este tipo de redes. Ahora analizaremos algunos otros:

### IV.4.A. I) FILTRADO DE DIRECCIONES MAC

Este método consiste en crear una tabla de direcciones MAC de los dispositivos inalámbricos autorizados en cada punto de acceso, para comunicarse exclusivamente con ellos. Filtrando así los dispositivos autorizados y desechando los demás.

Tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee desventajas para uso en redes medianas o grandes:

- No es escalable. Cada vez que se desee autorizar o dar de baja un equipo, es necesario actualizar las tablas. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.
- El formato de una dirección MAC no es amigable, consta de 12 dígitos en hexadecimal, lo que puede llevar a cometer errores al teclearlos.
- Las direcciones MAC viajan sin cifrar por el aire. Un atacante puede capturarlas empleando un sniffer como AirJack[7] o WellenReiter[8] (Ver Anexo F), y usarla para hacerse pasar por un cliente válido.
- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. Si el equipo robado es un punto de acceso el problema es mayor, ya que contiene la tabla de direcciones MAC en su chip memoria.

Es un mecanismo burdo, básico y fácilmente descifrable por un experto, pero mantendrá a los usuarios inexpertos al margen.

---

[7] *AirJack*. "Wi-Fi Protected Access - Overview". URL: http://802.11ninja.net/airjack/
[8] *AirJack*. "*Wellenreiter* - WLAN Hacking". URL: http://www.wellenreiter.net/

## IV.4.A. II) VPNS - REDES PRIVADAS VIRTUALES

Aunque las tecnologías IPSec y VPN pueden ser utilizadas para proveer un grado de seguridad en el enlace inalámbrico de redes 802.11, esas tecnologías no fueron diseñadas específicamente para redes inalámbrica y por ello, son deficientes en varias áreas cuando son usadas para asegurar redes WLAN´s. Las redes basadas en IPSec tanto de Microsoft como IPSec-VPN, comúnmente usado y ofrecido en los productos de la compañía Cisco, tiene los siguientes problemas:

- Se requieren clientes VPN en cada equipo inalámbrico para ejecutar la autenticación y encriptación. Esto limita a los nodos a aquellos dispositivos que son soportados por los productos específicos de VPN a ser utilizados. Dispositivos tales como impresoras inalámbricas y otros dispositivos parecidos pueden no tener soporte de una solución VPN. En este caso, ninguna comunicación dirigida a estos aparatos podrá ser protegida por la encriptación VPN y por lo tanto vulnerable.
- Costosas ya que su configuración, implementación y mantenimiento requiere de recursos humanos con altos conocimientos técnicos para asegurar que el ambiente es seguro y accesible por los prospectos confiables.
- Desempeño, Interoperabilidad y Escalabilidad.
- No soportan movilidad, ni clientes DOS (Ej. Lectores de códigos de barras), ni PDAs.
- Tampoco soporta otros protocolos como IPX, NetBIOs ó AppleTalk.
- Uso de translación de direcciones de red (NAT - Network Address Translation)
- Las soluciones VPN no soportan multicasting, comunicación de una fuente a muchos usuarios en una red, la cual es utilizada en aplicaciones de audio y video.
- Las soluciones de capa 3 (VPN) tampoco protegen tramas de diseminación extensa (broadcast), exponiendo a la WLAN a un ataque de DoS por envenenamiento arp (Ver Glosario).

La seguridad en redes es mas apropiada cuando se implemente al nivel más bajo posible de las capas del modelo OSI, como se muestra en la Figura IV- 5.

Algunos productos comerciales y el 802.11i fueron diseñados para trabajar en la capa 2 del modelo OSI, específicamente para WLANs. IPSec, un protocolo de seguridad Red a Red, fue diseñado para trabajar en la capa 3 y diseñado para redes cableadas.

Las VPNs no son suficientes para proteger redes inalámbricas. Vea la Figura IV - 5, para entender lo que protege cada capa del modelo OSI.

Entre más alta sea la capa en la que la encriptación es implementada, más expuesta es la información a un ataque externo.

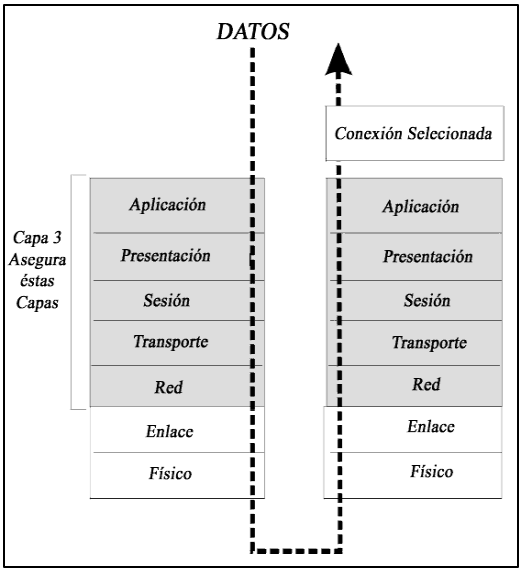



FIGURA IV- 5. SEGURIDAD A NIVEL CAPA 2

Las WLANs tienen su mayor debilidad en la capa 2. En la Figura IV-6 se tiene un comparativo de cómo es protegida la información a nivel paquete de datos.

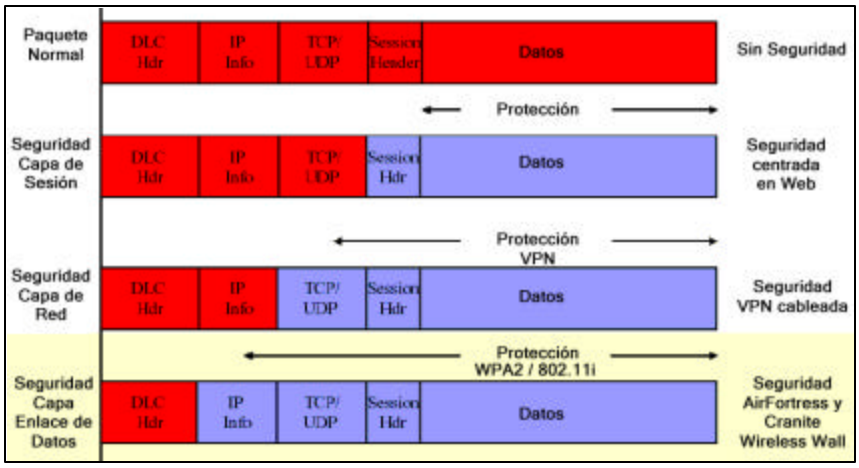



FIGURA IV- 6. NIVELES DE PROTECCIÓN EN LAS CAPAS DEL MODELO OSI

Por otro lado uno se puede preguntar ¿Para qué el IEEE invirtió más de 3 años de trabajo en el protocolo de seguridad 802.11i, si las VPNs ya estaban disponibles desde mucho antes? La respuesta es la misma, no protegen a las WLAN adecuadamente, adicionalmente los clientes pierden movilidad y el costo total de propiedad, TCO (Total Cost of Ownership), es mayor con VPNs que implementar WPA2, el cual, hasta la fecha no ha reportado ningún ataque exitoso, a excepción del ataque de negación de servicio, DoS, que sigue siendo un problema tanto para redes inalámbricas y cableadas.

## RESUMEN DE MÉTODOS BÁSICOS Y FALIBLES DE SEGURIDAD

| MÉTODO | BREVE DESCRIPCIÓN DE SU PROBLEMÁTICA |
|---|---|
| **SSID** | Aún cuando sea deshabilitado, la WLAN puede ser ubicada y atacada. |
| **FILTRO DE MACS** | Robo de una MAC legítima. Solo para uso en ambientes pequeños. |
| **WEP** | Método quebrantado por su débil diseño e implementación. |
| **WPA-PSK** | Quebrantado durante el intercambio de claves en texto claro y débil ante ataques de diccionario y de fuerza bruta. Herramienta: Aircrack y Airdecap. |
| **VPN** | Norma aplicable a redes cableadas que solo asegura de las capas 3 a la 7 del modelo OSI. Las WLAN pueden ser atacadas en la capa 2. |
| **EAP - LEAP** | Herramientas específicas (Asleap) hacen de este método algo muy sencillo de romper (1/10 WEP). Propietario de Cisco - posee 46% del mercado WiFi. |
| **EAP - FAST** | Reemplazo de LEAP pero incompatible con él. Usa un archivo de seguridad para cada usuario. Difícil de manejar, escalar e inseguro. |

TABLA IV - 3. MÉTODOS INSEGUROS UTILIZADOS EN WLANS.

Todos éstos métodos (Vea la Tabla IV-3) son una verdadera falacia en cuanto a seguridad se refiere y son obviamente inadecuados para proteger una WLAN apropiadamente. Muchos autores recomiendan su uso, algunos de ellos bajo el argumento de "más vale una seguridad débil a no tener seguridad alguna", la cual comparto parcialmente, ya que por falta de información mucha gente no activa un mejor nivel de seguridad en sus equipos. Mientras que algunos expertos de Tecnologías de la Información, creen tener perfectamente segura una red inalámbrica al utilizar alguno de estos métodos, en realidad tienen una red vulnerable.

La intención de mencionar estos métodos inseguros es la de advertir su alto riesgo al utilizarlos y así no tener una falsa sensación de seguridad, cuando en realidad lo que se tiene es un grave problema que puede afectar a la empresa en su totalidad.

## IV.4.B) ESTÁNDARES CONFIABLES DE SEGURIDAD PARA WLANS

Tanto la especificación WPA2 de la Alianza Wi-Fi, como estándar 802.11i de la IEEE solucionan todos los problemas conocidos de WEP y en estos momentos, se consideran soluciones fiables para proteger las WLANs, también denominada tecnología Wi-Fi.

Estas soluciones, WPA2 y 802.11i, implican la renovación completa de la plataforma de hardware instalada debido a su nuevo algoritmo de encriptación y a los nuevos protocolos utilizados.

La ventaja de WPA es que no requiere de actualizaciones de hardware en los equipos. Mientras no se descubran problemas de seguridad en WPA, esta implementación puede ser suficiente. Es posible ir integrando paulatinamente, nuevos equipos con mayores niveles de seguridad y así lograr, eventualmente, una red con seguridad robusta. Esto permite formular un plan de acción de mediano a largo plazo para logarlo.

Considere actualizar su equipo para que cumpla con el estándar 802.11i. Esto lo podrá hacer buscando los nuevos equipos denominados 802.11g, los cuales, además de integrar la nueva seguridad también incrementan la velocidad de las comunicaciones.

En el Apéndice F y en la Tabla IV-1 se ven las herramientas que un atacante (hacker) utiliza. Úselas, si logra penetrar su propia red vea donde están sus fallas y reconfigure su red para hacerla cada vez más segura.

## IV.4.C) RECOMENDACIONES DE SEGURIDAD PARA WLANS

En base a todo lo expuesto en este trabajo se ha elaborado la siguiente guía de recomendaciones y opciones de seguridad. Éstas se pueden dividir en:

- Redes Caseras o para Pequeños Negocios: SoHo[9]:
- Redes Empresariales

## IV.4.C. I) PARA OFICINAS PEQUEÑAS O CASERAS: SOHO

1) Averigüe si su equipo puede usar o es compatible con WPA o WPA2. Si lo es actívelo y utilice WPA-PSK con una contraseña de al menos 20 dígitos en cada uno de los dispositivos inalámbricos.
2) De no tener la opción de WPA, al menos active WEP.
3) Configure su Punto de Acceso para que solo acepte la dirección MAC de su(s) dispositivos inalámbricos.
4) De ser posible deshabilite la emisión del SSID de su Punto de Acceso y límite el área de cobertura.
5) Monitoree su red y vea quién esta conectado (Vea el Anexo F o la Sección IV.2).

[9] SoHo - Oficina pequeña - Oficina o red casera (Small Office - Home Office).

## IV.4.B. II) PARA WLANS EMPRESARIALES

1) Como mínimo utilice las consideraciones hechas para SoHo.
2) Implemente WPA2 u 802.11i. Lo cual requiere de servidores de autentificación que puedan brindar escalabilidad y autenticación. Como lo son los servidores: Windows 2003 de Microsoft, Odyssey de Funk Software y AEGIS de Meeting House.
3) Capacite a su personal en cuanto a seguridad informática.
4) Implementación de las actualizaciones de software/firmware que se liberen.
5) Este al tanto de los actuales y nuevos estándares de seguridad establecidos por la IEEE, la Alianza Wi-Fi y la organización ISO a través de sus páginas Web.
6) Desarrolle una política de seguridad y déla a conocer a todo su personal.
    a. Lineamientos para las contraseñas
    b. Monitoreo constante de su red. Atáquela, si puede entrar otros también
    c. Uso de bitácoras que nos muestren quien hizo que y cuando
    d. Acciones a tomar en caso de piratería
7) Hay que hacer frente a otras vulnerabilidades que se suman al incorporar una red inalámbrica a nuestra red cableada y sobre todo si se tiene conectividad a Internet: Virus, Troyanos, Spyware, Hackers, “hoyos” en los servicios y productos de los fabricantes de software, negligencia de los fabricantes y todas las vulnerabilidades relacionadas con los servicios IP.
8) Si un equipo inalámbrico es robado o algún miembro de su personal ha dejado la empresa con una computadora portátil, no corra riesgos, borre dicho usuario de su servidor de autenticación y de su red. De ser necesario cambie las contraseñas correspondientes.
9) De ser posible controle la Intensidad de la emisión inalámbrica y su cobertura.
10) Mantenga su(s) red(es) inalámbrica(s) en segmentos de red independientes.
11) Control de tráfico entre segmentos de red usando firewalls.
12) Este al pendiente de los descubrimientos de los hacker, ellos aman publicar sus logros. Busque en Internet cuales son y tome las medidas pertinentes.

# IV.5) MAYORES REQUERIMIENTOS DE SEGURIDAD INALÁMBRICA

## IV.5.A) REQUERIMIENTOS MAYORES AL 802.11I: DOD 8100.2

El Departamento de la Defensa de los Estados Unidos (DoD[10]) publicó la directiva DoD 8100.2, el 14 de Abril del 2004. Establece los estándares, de los militares de los Estados Unidos, al emplear dispositivos inalámbricos, tecnologías y servicios comerciales en sus aplicaciones sensitivas pero no clasificadas (SBU[11]) para sus redes de información global DoD GIG[12].

La directiva DoD 8100.2 debe ser certificada por el estándar FIPS 140-2. El cual, obliga el uso de AES y EAP-TLS, entre otras muchas cosas, para procesamiento de Información en agencias del gobierno Federal de los Estados Unidos (FIPS - US Federal Information Processing Standard).

El 802.11i permite el uso de alguno de los métodos EAP, incluyendo aquellos de los cuales se sabe que tienen problemas. Siendo esto una de las razones por las que esta directiva ha sido creada.

Una análisis imparcial de productos de hardware y software para redes inalámbricas que esta siendo utilizado con productos de encriptación militar para proveer radiocomunicación de redes inalámbricas a la milicia estadounidense con comunicaciones móviles de alta velocidad muestra que las soluciones más comunes son túneles VPN-IPSec (Capa 3) o soluciones de encriptación de Capa 2 para reunir los requisitos de seguridad de la información solicitados por FIPS 140-2.

Un estudio de dos soluciones líderes de hardware (Cisco) y software (AirFortress y Cranite WirelessWall) concluyó que una solución de capa 2 es por mucho superior a IPSec en una instalación inalámbrica. Para mayor información respecto a este análisis consulte las páginas de Web: http://www.airdefense.net y http://www.ngc.com.

Como notas finales hay decir que el Departamento de Defensa de los Estados Unidos tiene como política no usar redes inalámbricas para sus redes “clasificadas”. Las redes no clasificadas utilizan los productos AirFortress, Cranite WirelessWall y AirDefense que les permiten tener un muy buen nivel de seguridad, monitoreo, detección de intrusos y aplicación de políticas de seguridad.

[10] DoD - Department of Defense. Departamento de la Defensa de los Estados Unidos.
[11] SBU - Sensitive but Unclassified. Sensitivas pero no confidenciales.
[12] GIG - Global Information Grid. Red global de información.

## IV.5.B) PRODUCTOS COMERCIALES QUE BRINDAN SEGURIDAD A WLANS

En la Tabla IV-4 se muestras algunas de las soluciones comerciales existentes para elevar la seguridad de la red inalámbrica, su monitoreo y la aplicación de políticas de seguridad.

| PRODUCTO | DETALLES |
|---|---|
| Airfortress | Empresa dedicada a incrementar la seguridad tanto de sistemas operativos como de redes inalámbricas. Encriptación en Capa 2, monitoreo, alarmas y aplicación de políticas de seguridad. |
| AirDefense | Usa una arquitectura distribuida de sensores remotos y un servidor centralizado para monitorear constantemente toda la actividad inalámbrica en tiempo real, permitiendo a la empresa el control del espacio aéreo inalámbrico, definir y efectuar el cumplimiento de la política para los dispositivos inalámbricos y proveer análisis y detección de puntos de acceso falsos (rogue), protección de intrusiones, soporte operacional y monitoreo 24x7 saludable. |
| Cranite WirelessWall | Permite movilidad rápida entre puntos de acceso, soporta cualquier protocolo de capa 3, establece una relación de confianza entre los dispositivos inalámbricos y la compuerta (gateway) de seguridad al utilizar certificados PKI (X.509v3) y EAP-TTLS. Encripta a nivel Capa 2. |
| Orinoco | Fabricante líder de equipo inalámbrico que integra Monitoreo y Escaneo en sus puntos de acceso. |
| Airmagnet | Empresa desarrolladora de herramientas para la administración y gestión de redes wireless, ha anunciado su tercer generación de productos. La suite Mobile 3.0 - Airmagnet Laptop "Trio" y Airmagnet Handheld 3.0- añaden 22 nuevos dispositivos para mejorar el soporte y monitoreo para 802.11g. Además incluyen una nueva protección contra ataques de Denegación de Servicio. Otra novedad es "AirMagnet Reporter" que presenta los datos capturados por los productos móviles en el formato que el usuario desea. Asimismo se puede detectar intrusos , solucionar todo tipo de problemas en las redes inalámbricas y controlar la aplicación de las políticas de seguridad. |
| Funk Software | Tecnología y productos líderes en la protección de accesos remotos cableados o inalámbricos. Su gama de productos incluye un Servidor RADIUS/AAA que soporta accesos wireless según el estándar 802.1x y que, además, es compatible con EAP/TLS, EAP/TTLS, EAP/LEAP, EAP/PEAP y con WPA Y WPA2. Asimismo, es muy exitoso su cliente Odyssey para redes WiFi que es multiplataforma y multiprotocolo. |

TABLA IV- 4. OPCIONES COMERCIALES DE SEGURIDAD PARA WLANS.

Si se tiene la posibilidad de adquirir productos comerciales, adicionalmente a los estándares de seguridad, que brinden un nivel de seguridad adecuado a sus requerimientos, valórelos; su adquisición no es un gasto es una inversión en seguridad.

Cuando se evalúa una solución inalámbrica que satisfaga nuestras necesidades es muy importante tener en cuenta los estándares y tecnologías de más penetración, así como seleccionar productos bajo la certificación de la Alianza Wi-Fi. Esta sabia decisión ahorrará dinero, tiempo y problemas de incompatibilidad y nos brindará comunicación rápida, eficiente y segura.

# CONCLUSIONES

Durante el desarrollo de este trabajo se han planteado los conceptos básicos de las redes inalámbricas, los beneficios que brindan, los diferentes factores de seguridad que enfrentan. Se ha hecho un repaso de la evolución de los estándares de seguridad y las diferentes etapas que han seguido y se han explicado los diferentes mecanismos con que se cuenta hasta nuestros días para tener una red inalámbrica segura.

Se han mostrado además, las herramientas con las que cuenta un atacante para escuchar las transmisiones inalámbricas que viajan por el aire y como logran tener acceso a la red inalámbrica. No solo esto, sino adicionalmente rompen la seguridad provista por WEP. De tal modo que si nuestra red inalámbrica esta conectada a nuestra red cableada también están en riesgo los datos, infraestructura e información de nuestra red corporativa.

Hay que hacer frente a otras vulnerabilidades que se suman al incorporar una red inalámbrica a nuestra red cableada y sobre todo si se tiene conectividad a Internet: Virus, Troyanos, Spyware, Hackers, "hoyos" en los servicios y productos de los fabricantes, negligencia de los fabricantes y todas las vulnerabilidades relacionadas con los servicios IP.

Todo lo anterior me permite concluir que las redes inalámbricas son altamente vulnerables de no estar configuradas apropiadamente en cuanto a seguridad. Por lo que esto es un aspecto crítico que no se puede ni se debe descuidar, considerando aspectos como autenticidad del usuario, privacidad de la información e integridad de la misma.

Se ha mostrado en el segundo capítulo que WEP, el primer mecanismo de seguridad del IEEE 802.11, tiene muchas vulnerabilidades documentadas y es inseguro. Por lo cual, no debe ser considerado como una opción real de seguridad para las redes inalámbricas.

Estar a la vanguardia requiere de la capacitación del personal encargado de las Tecnologías de la Información, así como el desarrollo e implementación de políticas de seguridad para la empresa son de vital importancia. Adicionalmente, las redes inalámbricas han introducido un nuevo lenguaje a la hora de hablar de redes de datos. Poder identificar correctamente la gran cantidad de nuevas siglas y acrónimos es una ventaja importante a la hora de discutir una propuesta concreta.Esto nos permitirá conocer: el equipo que se tiene o que se va a adquirir, como configurarlo, activar las opciones más recientes de seguridad, administrarlo y monitorearlo. Ya que el gran desconocimiento en seguridad inalámbrica por parte de los usuarios y empresas es algo asombroso y alarmante debido a que no se conocen los riesgos de un punto de acceso mal configurado o sin seguridad. Adicional e increíblemente existen proveedores que continúan ofreciendo productos con seguridad WEP, aún cuando son ampliamente conocidas sus fallas.

Al adquirir productos certificados por la Alianza Wi-Fi, no debe darse por hecho que al hacerlo es ya de por si un producto seguro, ya que hay que configurarlo apropiadamente. Lo que si garantizamos es su compatibilidad, interconectividad y funcionalidad gracias a las pruebas a las que ha sido sometidos.

El estándar de facto, WPA2, de la alianza Wi-Fi y el estándar 802.11i desarrollado por la IEEE más recientemente, son las opciones empresariales a seguir en seguridad inalámbrica. Y que el WPA-

PSK (con una clave de 20 caracteres ó más) y el filtro de direcciones MAC sería lo apropiado para redes caseras o para pequeñas empresas que no cuenten con suficientes recursos.

En cuanto a los hackers, visto desde una perspectiva personal, concluyo que son gente sagaz, con alta capacidad intelectual y vastos conocimientos de cómputo. Ponen a prueba los sistemas de seguridad desarrollados. Colaboran en establecer una seguridad mayor al romper la existente. Uno de sus mayores y mejores aspectos es el hecho de que les agrada sobremanera comentar sus logros, es decir, son un buen parámetro para determinar si la seguridad implementada es adecuada y suficiente. Es recomendable visitar sus sitios de Web o los de noticias tecnológicas para estar al tanto de sus hallazgos.

Finalmente la seguridad informática y particularmente en las redes inalámbricas de una empresa o corporación debe ser un asunto primordial ya que de esto depende, en muchas ocasiones, su éxito o fracaso. Contratar especialistas o empresas expertos en seguridad no es un gasto, es más bien, una inversión.

Las investigaciones realizadas para la elaboración de esta tesina han enfrentado varias dificultades:

1) Libros y publicaciones con serias fallas en cuanto a su contenido.
2) Internet es una increíble herramienta y fuente de información, sin embargo no todo lo que se publica ahí es fidedigno.
3) Costos elevados para acceso a los “White Papers”.

Para la realización de esta tesina, así como para mi vida profesional han sido de gran ayuda muchas de las materias que curse durante mis estudios profesionales, por mencionar algunas: Arquitectura de Computadoras, Métodos Numéricos, Optimización, Ensambladores, Probabilidad, Estadística, Teleprocesos, Bases de Datos, Estructura de Datos y Análisis de Algoritmos.

Debo mencionar que seria un gran aporte para la carrera de Matemáticas Aplicadas y Computación incluir materias tales como redes de computo, ruteo, seguridad informática, alta dirección, análisis financiero, administración de recursos financieros y humanos, etc., así como laboratorios de cómputo mejor equipados. Realizar intercambio de estudios con otras universidades a nivel internacional llevando a cabo alianzas y programas de certificaciones con compañías comerciales. Difundiendo esto ampliamente para promover el interés y así plantear una serie de alternativas para toda la comunidad universitaria.

Independiente a todo esto, seria de gran ayuda el contar con talleres donde se planteen aspectos de lo que es un proyecto de vida para complementar el aspecto humano que todos tenemos, y no solamente brindar materias relacionadas a la carrera.

Me permito mencionar todo esto ya que personalmente enfrenté, sin las herramientas adecuadas, durante mi desarrollo profesional, muchos de estos retos y aspectos. Pienso que serian de gran ayuda para nuestros nuevos estudiantes y que les brindarían los elementos necesarios para enfrentar los nuevos retos tanto profesionales como humanos.

# ANEXOS

## SEGURIDAD EN REDES INALÁMBRICAS (WI-FI)

# ANEXO A

## ASPECTOS FUNDAMENTALES DE LA FRECUENCIA

El concepto de frecuencia es más fácil de entender a través de la analogía de los patrones de olas que se crean después de arrojar un objeto en el agua; primero considere el contexto de la frecuencia de radio difusión de Maxwell. Las olas emanan hacia fuera con un forma específica desde el punto donde el objeto cayó en el agua. Las olas se debilitan en cuanto a energía a medida que se alejan del punto donde el objeto entró al agua, y también cambian de forma conforme se alejan del centro. Estas olas se conocen como ***ondas senoidales*** debido a la forma que tienen.

Las ondas senoidales salen de una antena transmisora de manera semejante a cuando las olas emanan del punto en que la piedra cae al agua. El número de veces por segundo que una onda senoidal se crea desde la antena transmisora (o se recibe en la antena receptora) es la **frecuencia**. La unidad básica de tiempo que se usa en relación con la frecuencia es el "**hertz**".

Las ondas senoidales están controladas en términos de amplitud, frecuencia y fase. Este control se conoce como ***modulación***, que tiene un efecto significativo en la salida de datos y otros atributos RF importantes. Este "control" se efectúa a través de la ejecución de diseños de ingeniería muy específicos, mismos que se relacionan con la selección de componentes eléctricos en particular.

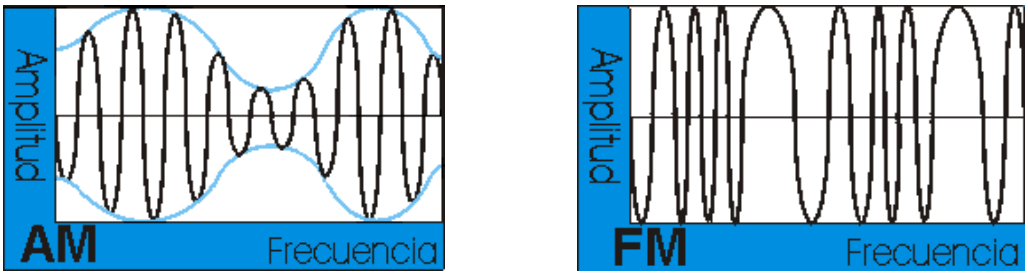



FIGURA A-1. MODULACIÓN AM Y FM

Las características de una onda de RF (Radio Frecuencia) son muy distintas en los diferentes puntos del espectro electromagnético. Por lo común entre más alta sea la frecuencia será más corta la distancia de transmisión para una potencia determinada y más importante el aspecto de las trayectorias múltiples. Los sistemas RF poseen dos categorías amplias: longitudes de onda menor a 10 GHz (microondas) y longitudes de onda mayores a 10 GHz (milimétricas). Cada una de ellas tiene ciertas ventajas y desventajas como se resumen en la Tabla A-1:

| Característica | Microondas | Onda Milimétrica |
|---|---|---|
| Frecuencia de radio | < 10 GHz | > 10 GHz |
| Costo | Menos que la Onda Milimétrica | Más que las microondas |
| Complejidad | Menos que la Onda Milimétrica | Mayor a las microondas |
| Rango Nominal | 5 - 20 millas | < a 5 millas |
| ¿Le afecta el clima? | Normalmente no | Normalmente si |
| Uso típico | Multipunto | Punto a punto |
| ¿Representan un problema las trayectorias múltiples? | Si | Generalmente no |
| ¿Requieren licencia? | Generalmente | Generalmente |

TABLA A-1. BREVE COMPARACIÓN DE LAS MICROONDAS Y LAS ONDAS MILIMÉTRICAS.

Una señal RF típica que se envía entre dos sitios es, con frecuencia, 10 000 veces más débil que eso; no obstante, sorprendentemente es muy aprovechable y en realidad es algo que ocurre en forma regular.

La energía que se pierde durante el tiempo en que se transmite entre dos puntos se conoce como ***pérdida de propagación*** *o* ***pérdida de propagación en el espacio libre***. Lo importante aquí es que ésta es constante a lo largo de una ruta determinada, sin importar la cantidad de potencia usada por el transmisor; por lo cual, las variaciones debidas a la modulación se pueden reproducir suficientemente fiel en el receptor.

## MODULACIÓN

Cualquier señal que se puede traducir en una forma eléctrica, como audio, video o datos, se pude modular y enviar a través del aire.

La modulación es la técnica de convertir los bits en algo que se transmite a través de la frecuencia portadora de la onda y a través del aire. La frecuencia portadora de la onda no tiene inteligencia; los datos modulados contienen la inteligencia. La frecuencia portadora de la onda de un radio 802.11b y 802.11g es de 2.4 GHz a 2.485 GHz en Estados Unidos.

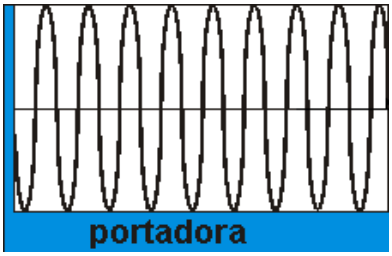



FIGURA A-1. ONDA PORTADORA

La frecuencia portadora no transporta por si misma la información, sino que ésta viaja a través de la frecuencia portadora, de ahí el significado del término. Para ejemplificar esto: si se estuviera usando una impresora, la frecuencia portadora de la onda sería el papel y la información modulada serían las letras en el papel.

Existen muchos esquemas de modulación distintos; la Tabla A-2 contiene una lista parcial.

| Descripción de Frecuencia | Rango de Frecuencia | Longitud de onda en el espectro de extremo inferior |
|---|---|---|
| Muy baja (VLF) | 0 KHz - 30 Khz | 100 Km |
| Baja (LF) | 30 KHz - 300 Khz | 10 Km |
| Intermedia (MF) | 300 KHz - 3 Mhz | 1 Km |
| Alta (HF) | 3 MHz - 30 Mhz | 100 metros |
| Muy alta (VHF) | 30 MHz - 300 Mhz | 10 metros |
| Ultra alta (UHF) | 300 MHz - 3 Ghz | 1 metro |
| Súper alta (SHF) | 3 GHz - 30 Ghz | 100 metros |
| Extremadamente alta (EHF) | 30 GHz - 300 Ghz | 10 metros |

TABLA A-2. FRECUENCIAS DE ACUERDO CON LA DEFINICIÓN DEL GOBIERNO DE ESTADOS UNIDOS

Todos los esquemas están relacionados con uno de los tres tipos de modulación más importantes:

**MODULACIÓN DE AMPLITUD**

La potencia de salida del transmisor es variable, mientras que la frecuencia y la fase de la onda senoidal permanecen constantes.

**MODULACIÓN DE FRECUENCIA**

La potencia de salida y fase permanecen constantes en tanto que la frecuencia varía de acuerdo con un rango pequeño.

**MODULACIÓN DE FASE**

La amplitud y la frecuencia permanecen constantes, pero la fase dentro de la frecuencia portadora de la onda cambia respecto a un rango pequeño.

A continuación, en la Tabla A-3, se listan algunas de los esquemas de modulación más importantes:

| Símbolo | Esquema de modulación |
|---|---|
| AM | Amplitud |
| FM | Frecuencia |
| SSB | Banda lateral única |
| PM | Fase |
| CCK | Codificación Complementaria |
| CW | Onda continua (telegrafía) |
| PCM | Codificación de pulsos |
| VSB | Banda lateral residual |
| BMAC | Componentes analógicos de multiplexión de ondas tipo B |
| QAM | Amplitud del cuadrante |
| DSSS | Espectro extendido de secuencia directa |
| FHSS | Espectro extendido de salto de frecuencia |
| BFSK | Modulación de frecuencia por desplazamiento binario |
| PBCC | Codificación compleja de paquetes binarios |
| QPSK | Modulación de fase por desplazamiento en cuadrante |

TABLA A-3. DISTINTOS ESQUEMAS DE MODULACIÓN

En general los esquemas de modulación más comunes son: BFSK o FSK, Modulación por fase por desplazamiento binario (Binary Phase Shift Keying), QPSK y QAM.

# ANEXO B

# OFDM

La modulación por división ortogonal de frecuencia, en inglés Orthogonal Frequency Division Multiplexing (OFDM), es una modulación que consiste en enviar la información modulando en QAM o en PSK. OFDM divide la señal de radio en muchas sub-señales que son transmitidas simultáneamente hacia el receptor en diferentes frecuencias. Este *espaciamiento* o división provee la "ortogonalidad". OFDM reduce la diafonía (efecto de cruce de líneas) durante la transmisión de la señal.

Con esta técnica se previene a los demoduladores ver frecuencias que no sean las suyas. Los beneficios de OFDM son alta eficiencia espectral, resistencia a la interferencia de Radio Frecuencia y baja distorsión. Debido a la las características de esta modulación, las distintas señales con distintos retardos y amplitudes que llegan al receptor contribuyen positivamente a la recepción (Figura A-1), por lo que existe la posibilidad de crear redes de radiodifusión de frecuencia única sin que existan problemas de interferencia. Esta técnica permite transmitir grandes cantidades de datos digitales sobre una onda de radio.

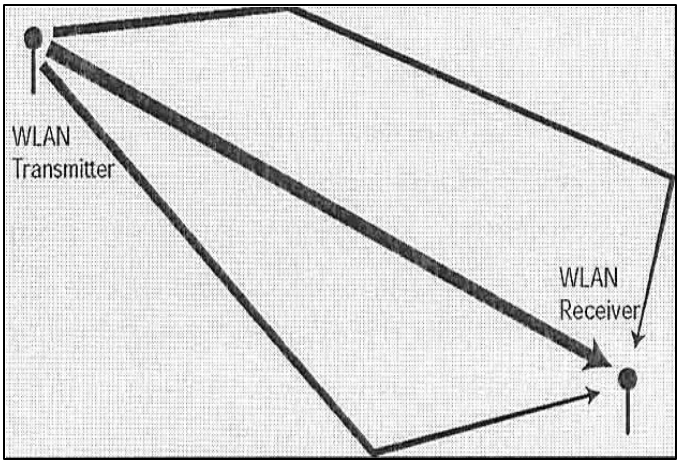



FIGURA B-1. SEÑALES DE RADIO VIAJANDO SOBRE RUTAS MULTIPLES.

La tecnología fue primero concebida en 1960 y 1970 durante la investigación para minimizar la interferencia entre canales cercanos en frecuencia.

En algunos aspectos, OFDM es similar a la multiplexación de división de frecuencias convencionales (FDM). La diferencia esta en la forma en la que las señales son moduladas y demoduladas. La prioridad es dada a minimizar la interferencia o comunicación cruzada, en los canales y símbolos que componen los datos. Menor importancia es puesta en perfeccionar canales individuales.

La FDM (Frequency division multiplexing) es una tecnología que transmite señales múltiples simultáneamente sobre un canal de transmisión, tal como un sistema cableado. Cada señal viaja dentro de su propio rango de frecuencia (portadora), la cual es modulada por los datos (texto, voz, video, etc).

Entre los sistemas que usan la modulación OFDM destacan:

La televisión digital terrestre DVB-T, también conocida como TDT
La radio digital DAB
La radio digital de baja frecuencia DRM
El protocolo de enlace ADSL
El protocolo de red de área local IEEE 802.11a/g, también conocido como Wireless LAN
El sistema de transmisión inalámbrica de datos WiMAX
Es una técnica de modulación usada para TV digital en Europa, Japón y Australia.

# ANEXO C

# EL MODELO OSI

El Modelo de Referencia de Interconexión de Sistemas Abiertos, OSI-RM (Open System Interconection-Reference Model), proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial.

Para poder simplificar el estudio y la implementación de la arquitectura necesaria, la ISO dividió el modelo de referencia OSI en capas, entendiéndose por **capa** una entidad que realiza de por sí una función específica.

Cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI.

Los criterios que llevaron a este modelo de referencia fueron:

- Creación de una nueva capa siempre que se precise un nuevo grado de abstracción.
- A cada capa deberá asignarse un número bien definido de funciones propias.
- La funcionalidad de cada capa deberá tener en cuenta la posibilidad de definir protocolos normalizados a nivel internacional.
- La frontera de las capas será tal que se minimice el flujo de información a través de la interfaz entre ambas.
- El número de capas será lo suficientemente grande como para no reunir en un nivel funcionalidades distinta y lo suficientemente pequeño para que el resultado final sea manejable en la práctica.

En el modelo de referencia OSI hay siete capas, cada una de las cuales ilustra una función de red particular. La división de la red en siete capas presenta las siguientes ventajas:

1. Divide la comunicación de red en partes más pequeñas y sencillas.
2. Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
3. Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida. Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.
4. Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

Una analogía del sistema de capas puede ser la forma en que una carta es enviada desde el emisor hasta el destinatario. En este proceso intervienen una serie de entidades o capas (carteros, oficinas postales, medios de transporte, etc.), cada una de las cuales realiza una serie de funciones específicas, necesarias para el funcionamiento de las demás y para la entrega efectiva de la carta.

Las sietes capas del modelo OSI son:


FIGURA C-1. CAPAS DEL MODELO OSI

## CAPA 7: LA CAPA DE APLICACIÓN

La capa de aplicación es la capa del modelo OSI más cercana al usuario, y está relacionada con las funciones de mas alto nivel, proporcionando soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales.

Es el medio por el cual los procesos las aplicaciones de usuario acceden a la comunicación por red mediante el entorno OSI, proporcionando los procedimientos precisos para ello.

Los procesos de las aplicaciones se comunican entre sí por medio de entidades de aplicación propias, estando éstas controladas por protocolos específicos de la capa de aplicación, que a su vez utilizan los servicios de la capa de presentación, situada inmediatamente debajo en el modelo.

Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo (procesadores de texto, hojas de cálculo, navegadores web, etc.).

La capa de aplicación establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

## CAPA 6: LA CAPA DE PRESENTACIÓN

La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo.

Su tarea principal es aislar a las capas inferiores del formato de los datos de las aplicaciones específicas, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red, entendible por todos los sistemas y apto para ser enviado por red.

Es también las responsable de la obtención y de la liberalización de la conexión de sesión cuando existan varias alternativas disponibles.

Para cumplir estas funciones, la capa de presentación realiza las siguientes operaciones:

- Traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. Para ello convierte los datos desde el formato local al estándar de red y viceversa.
- Definir la estructura de los datos a transmitir. Por ejemplo, en el caso de un acceso a base de datos, definir el orden de transmisión y la estructura de los registros.
- Definir el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc.).
- Dar formato a la información para visualizarla o imprimirla. Comprimir los datos si es necesario.
- Aplicar a los datos procesos criptográficos cuando sea necesario.

## CAPA 5: LA CAPA DE SESIÓN

La capa de sesión proporciona sus servicios a la capa de presentación, suministrando el medio necesario para que las entidades de presentación de dos hosts que se están comunicando por red organicen y sincronicen su diálogo y procedan al intercambio de datos.

Sus principales funciones son:

- Establecer, administrar y finalizar las sesiones entre dos hosts (máquinas en red) que se están comunicando.
- Si por algún motivo una sesión falla por cualquier causa ajena al usuario, restaurar la sesión a partir de un punto seguro y sin pérdida de datos o, si esto no es posible, terminar la sesión de una manera ordenada, comprobando y recuperando todas sus funciones, evitando así problemas en sistemas transaccionales.
- Sincronizar el diálogo entre las capas de presentación de los dos hosts y administrar su intercambio de datos, estableciendo las reglas o protocolos para el dialogo entre máquinas, regulando quien habla y por cuanto tiempo.
- Conseguir una transferencia de datos eficiente y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.
- Manejar **tokens**. Los tokens son objetos abstractos y únicos que se usan para controlar las acciones de los participantes en la comunicación, base de ciertos tipos de redes, como Token Ring o FDDI.
- Hacer **checkpoints**, que son puntos de recuerdo en la transferencia de datos, necesarios para la correcta recuperación de sesiones perdidas.

## CAPA 4: LA CAPA DE TRANSPORTE

La capa de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión.

Para ello, divide los datos originados en el host emisor en unidades apropiadas, denominadas **segmentos**, que vuelve a reensamblar en el sistema del host receptor.

Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones de usuario, las tres capas inferiores se encargan del transporte de datos. Además, la capa de transporte es la primera que se comunica directamente con su capa par de destino, ya que la comunicación de las capas anteriores es de tipo máquina a máquina.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísle las capas superiores de los detalles del mismo, encargándose de conseguir una transferencia de datos segura y económica y un transporte confiable de datos entre los nodos de la red. Para ello, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales, proporcionando un servicio confiable mediante el uso de sistemas de detección y recuperación de errores de transporte.

Se conocen con el nombre de **circuitos virtuales** a las conexiones que se establecen dentro de una red. En ellos no hay la necesidad de tener que elegir una ruta nueva para cada paquete, ya que cuando se inicia la conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el tráfico de datos posterior.

Podemos resumir las funciones de la capa de transporte en los siguientes puntos:

- Controlar la interacción entre procesos usuarios en las máquinas que se comunican.
- Incluir controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.
- Controlar el flujo de transacciones y el direccionamiento de procesos de maquina a procesos de usuario.
- Asegurar que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.
- Aceptar los datos del nivel de sesión, fragmentándolos en unidades más pequeñas aptas para el transporte confiable, llamadas segmentos, que pasa luego a la capa de red para su envío.
- Realizar funciones de control y numeración de las unidades de información (los segmentos).
- Reensamblar los mensajes en el host destino, a partir de los segmentos que lo forman.
- Garantizar la transferencia de información a través de la red.

## CAPA 3: LA CAPA DE RED

La capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de la mejor ruta para la comunicación entre máquinas que pueden estar ubicadas en redes geográficamente distintas.

Es la responsable de las funciones de conmutación y enrutamiento de la información (direccionamiento lógico), proporcionando los procedimientos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red (forma en que están interconectados los nodos), con objeto de determinar la ruta más adecuada.

Sus principales funciones son:

- Dividir los mensajes de la capa de transporte (segmentos) en unidades más complejas, denominadas **paquetes**, a los que asigna las direcciones lógicas de los host que se están comunicando.
- Conocer la topología de la red y manejar el caso en que la máquina origen y la máquina destino estén en redes distintas.
- Encaminar la información a través de la red en base a las direcciones del paquete, determinando los métodos de conmutación y enrutamiento a través de dispositivos intermedios (routers).
- Enviar los paquetes de nodo a nodo usando un circuito virtual o datagramas.
- Ensamblar los paquetes en el host destino.

En esta capa es donde trabajan los routers, dispositivos encargados de encaminar o dirigir los paquetes de datos desde el host origen hasta el host destino a través de la mejor ruta posible entre ellos.

## CAPA 2: LA CAPA DE ENLACE DE DATOS

La capa de enlace proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico.

Se ocupa del direccionamiento físico, la topología de red, el acceso a la misma, la notificación de errores, la formación y entrega ordenada de datos y control de flujo.

Su principal misión es convertir el medio de transmisión en un medio libre de errores de cualquier tipo, realizando para ello las siguientes funciones:

- Establecer los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.

- Agregar una secuencia especial de bits al principio y al final de los paquetes de datos, estructurando este flujo bajo un formato predefinido, denominado **trama**, que suele ser de unos cientos de bytes.

- Sincronizar el envío de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, se usan **CRC** (Códigos Cíclicos Redundantes) y envío de acuses de recibos positivos y negativos, y para evitar tramas repetidas se usan números de secuencia en ellas.

- Controlar la congestión de la red.

- Regular la velocidad de tráfico de datos.

- Controlar el flujo de tramas mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción.

- Encargarse del acceso de los datos al medio (soportes físicos de la red).

## CAPA 1: LA CAPA FÍSICA

La misión principal de esta capa es transmitir bits por un canal de comunicación, de manera que cuanto envíe el emisor llegue sin alteración al receptor.

La capa física proporciona sus servicios a la capa de enlace de datos, definiendo las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son transmitidos.

Sus principales funciones las podemos resumir en:

- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar voltajes y pulsos eléctricos.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

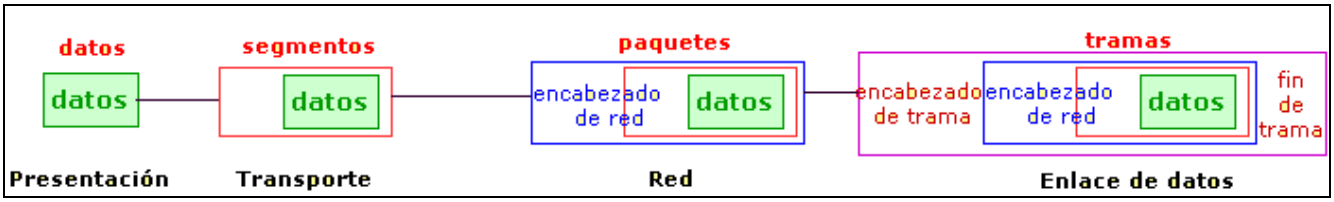
Esta capa solamente reconoce bits individuales.

## ENCAPSULAMIENTO

Si un computador A desea enviar datos a otro B, en primer término los datos a enviar se deben colocar en paquetes que se puedan administrar y rastrear, a través de un proceso denominado **encapsulamiento**.

Cuando las aplicaciones de usuario envían los datos desde el origen, estos viajan a través de las diferentes capas. Las tres capas superiores (aplicación, presentación y sesión) preparan los datos para su transmisión, creando un formato común para la transmisión. Una vez pasados a este formato común, el encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tráfico de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información.

El encapsulamiento consta de los cinco pasos siguientes:




1. **Crear los datos** (capa de presentación). Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la red.

2. **Empaquetar los datos** para ser transportados de extremo a extremo (capa transporte). Se dividen los datos en unidades de un tamaño que se pueda administrar (los segmentos), y se les asignan números de secuencia para asegurarse de que los hosts receptores vuelvan a unir los datos en el orden correcto. Luego los empaqueta para ser transportados por la red. Al utilizar segmentos, la función de transporte asegura que los hosts del mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.

3. **Agregar la dirección de red al encabezado** (capa de red). El siguiente proceso se produce en la capa de red, que encapsula el segmento creando un paquete o datagrama, agregándole las direcciones lógicas de red de la máquina origen y de la máquina destino. Estas direcciones ayudan a los ruteadores a enviar los paquetes a través de la red por una ruta seleccionada.

4. **Agregar la dirección local al encabezado** de enlace de datos (capa enlace de datos). En la capa de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama las direcciones MAC (número de la tarjeta de red, único para cada tarjeta) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

5. **Transmitir el tren de bits creado**. (Capa física). Por último, el tren de bits originado se transmite a la red a través de los medios físicos (cableado, ondas, etc.). Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio, que puede variar a lo largo de la ruta utilizada.

Cuando los datos se transmiten en una red de área local (red LAN), se habla de las unidades de datos en términos de tramas, debido a que la dirección MAC es todo lo que se necesita para llegar desde el

host origen hasta el host destino. Pero si se deben enviar los datos a un host de otra red interna o a través de Internet es necesario el uso de paquetes de datos que contengan las direcciones lógicas de las máquinas que se deben comunicar.
Las tres capas inferiores (red, enlace de datos, física) del modelo OSI son las capas principales de transporte de los datos a través de una red interna o de Internet.

## COMUNICACIÓN ENTRE CAPAS

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el lugar destino. Esta forma de comunicación se conoce como **comunicaciones de par-a-par**. Las reglas y convenciones que controlan esta conversación se denominan **protocolo de la capa n**, y se ocupan del formato y significado de las unidades de datos intercambiadas.

Durante este proceso, cada protocolo de capa intercambia unidades de información entre capas iguales de las máquinas que se están comunicando, conocidas con el nombre de **unidades de datos de protocolo** (PDU). Cada capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino.

También cada capa de un modelo o arquitectura de red recibe **servicios** a la capa que se encuentra debajo de ella y suministra servicios a la que está por encima en la jerarquía, siendo la implantación de estos servicios transparente al usuario. Hay dos tipos principales de servicios:

1. **Servicios orientados a la conexión**: En ellos la conexión es como un tubo a través del cual se envía la información de forma continuada, por lo que los mensajes llegan en el orden que fueron enviados y sin errores. Proporcionan un servicio confiable de comunicación de datos. Una analogía es el sistema telefónico.

2. **Servicios sin conexión**: En los que cada mensaje lleva la dirección completa de su destino, la información no se envía de forma continuada y el ruteo de cada mensaje es independiente. El servicio no es entonces confiable, pues la capa de red ni garantiza el orden de los paquetes ni controla su flujo, y los paquetes deben llevar sus direcciones completas de destino. Una analogía sería el caso del sistema de correo convencional.

Otra clasificación posible de los servicios en la que distingue entre confiables y no confiables:

- **Servicios confiables**: son aquellos en los que la transmisión de datos está controlada en cada momento, pudiéndose determinar el correcto envío y recepción de todos los datos transmitidos. Para ello la máquina receptora envía mensajes de acuse de recibo de las tramas recibidas a la máquina emisora.

- **Servicios no confiables**: en estos no existe un control de los datos transmitidos, por lo que no se puede garantizar que se hayan recibido todos los datos. Una forma de contrarrestar esta debilidad es la implementación de un sistema de acuse de recibo de las unidades de datos.

En realidad, una capa de una máquina no puede transferir los datos de forma directa a su capa par de otra, si no que necesita los servicios de todas las capas que se encuentran por debajo de ella en la jerarquía de capas, pasándose la información hacia abajo hasta llegar al nivel físico, que es el que realiza el proceso de transferencia de datos.

Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le puede agregar cualquier encabezado e información final que la capa necesite para ejecutar su función. De esta forma, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final adicionales.

La capa de red presta un servicio a la capa de transporte, trasladando esos datos a través de la red. Para ello encapsula los datos y les agrega un encabezado específico (direcciones lógicas origen y destino), con lo que crea un paquete (PDU de la Capa 3).

La capa de enlace de datos suministra un servicio a la capa de red. Encapsula la información de la capa de red (paquetes) en una trama (la PDU de la Capa 2), cuyo encabezado contiene la información necesaria (direcciones físicas) para completar las funciones de enlace de datos.
La capa física también suministra un servicio a la capa de enlace de datos, codificando los datos de la trama de enlace de datos en un patrón de unos y ceros (trenes de bits) para su transmisión a través del medio (generalmente un cable).

# ANEXO D

# PROTOCOLO TCP/IP

Aunque poca gente sabe lo que es TCP/IP todos lo emplean indirectamente y lo confunden con un solo protocolo cuando en realidad son varios, de entre los cuales destaca y es el más importante el protocolo IP. Bajo este nombre(TCP/IP) se esconde uno de los protocolos más usados del mundo, debido a que es el más usado por Internet y esta muy extendido en el sistema operativo UNIX.

En el 1973 , la DARPA inició un programa de investigación de tecnologías de comunicación entre redes de diferentes características. El proyecto se basaba en la transmisión de paquetes de información, y tenia por objetivo la interconexión de redes. De este proyecto surgieron dos redes: Una de investigación, ARPANET, y una de uso exclusivamente militar, MILNET. Para comunicar las redes, se desarrollaron varios protocolos: El protocolo de Internet y los protocolos de control de transmisión. Posteriormente estos protocolos se englobaron en el conjunto de protocolos TCP/IP.

En 1980, se incluyo en el UNIX 4.2 de BERKELEY, y fue el protocolo militar standard en 1983. Con el nacimiento en 1983 de INTERNET, este protocolo se popularizo bastante, y su destino va unido al de Internet. ARPANET dejo de funcionar oficialmente en 1990.

Algunos de los motivos de su popularidad son:

- Independencia del fabricante
- Soporta múltiples tecnologías
- Puede funcionar en maquinas de cualquier tamaño
- Estándar de EEUU desde 1983

La arquitectura de un sistema en TCP/IP tiene una serie de metas:

- La independencia de la tecnología usada en la conexión a bajo nivel y la arquitectura del ordenador
- Conectividad Universal a través de la red
- Reconocimientos de extremo a extremo
- Protocolos estandarizados

## ESTRUCTURA INTERNA

El modelo básico en Internet es el modelo Cliente/Servidor. El Cliente es un programa que le solicita a otro que le preste un servicio. El Servidor es el programa que proporciona este servicio.

La arquitectura de Internet esta basada en capas. Esto hace más fácil implementar nuevos protocolos. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura. El modelo de capas de TCP/IP es algo diferente al propuesto por ISO para la interconexión de sistemas abiertos .

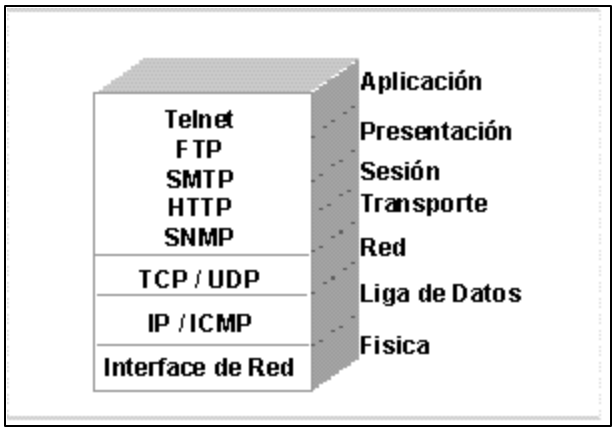



FIGURA D-1. RELACIÓN DEL MODELO TCP/IP CON EL MODELO OSI

## CAPAS

Los Protocolos TCP / IP se clasifican según la capa en la que trabajen.

Las capas son las siguientes:

**APLICACIÓN** - Telnet, FTP, SMTP, Http, SNMP, etc.

**TRANSPORTE** - TCP / UPD

**RED** - IP / ICMP

**FÍSICA** - Interfase de Red

## CAPA FÍSICA

Este nivel corresponde al *hardware*. En este nivel están los protocolos ARP y RARP.

**ARP**

El protocolo ARP (Address Resolution Protocol), es el encargado de convertir las direcciones IP en direcciones de la red física.

El funcionamiento del protocolo ARP es bastante simple. Cuando una máquina desea enviar un mensaje a otra máquina que está conectada a través de una red ethernet se encuentra con un problema: la dirección IP de la máquina en cuestión es diferente a la dirección física de la misma. La máquina que quiere enviar el mensaje sólo conoce la dirección IP del destino, por lo que tendrá que encontrar un modo de traducir la dirección IP a la dirección física. Esto se hace con el protocolo ARP.

Este protocolo utiliza una tabla denominada Tabla de Direcciones ARP, que contiene la correspondencia entre direcciones IP y direcciones físicas utilizadas recientemente. Si la dirección solicitada se encuentra en esta tabla el proceso se termina en este punto, puesto que la máquina que origina el mensaje ya dispone de la dirección física de la máquina destino.

Si la dirección buscada no esta en la tabla el protocolo ARP envía un mensaje a toda la red. Cuando un ordenador reconoce su dirección IP envía un mensaje de respuesta que contiene la dirección física. Cuando la máquina origen recibe este mensaje ya puede establecer la comunicación con la máquina destino, y esta dirección física se guarda en la Tabla de direcciones ARP.

**RARP**

El protocolo RARP (Reverse Address Resolution Protocol) es el encargado de asignar una dirección IP a una dirección física.
Algunos hosts, como por ejemplo estaciones de trabajo sin disco, desconocen su propia dirección IP cuando arrancan. Para determinarla, emplean un mecanismo similar al ARP, pero ahora el parámetro conocido es la dirección hardware el host y el requerido su dirección IP. La diferencia básica con ARP es el hecho de que debe existir un "servidor RARP" en la red que mantenga una base de datos con las direcciones hardware y las direcciones de protocolo respectivas.

## CAPA DE RED

Se encargan de ruteo de información a través de una red de área amplia. Existen dos protocolos en este nivel, uno de ellos conocido como IP (Internet Protocol) que es probablemente el protocolo de ruteo más utilizado y trabaja bajo el principio de direcciones enmascaradas; también existe una versión más simplificada de IP conocida como ICMP que se encarga de rutear paquetes sin ningún esquema de seguridad pero a mayor velocidad, se utiliza en particular para transmisión de e-mails.

## CAPA DE TRANSPORTE

La capa de Transporte de TCP/IP ofrece dos protocolos: TCP para redes orientadas a conexiones y UDP para redes no orientadas a conexión. Un complementario a cerca de las capas de transporte TCP y UDP es que a diferencia de OSI pueden trabajar a nivel local sin necesidad de enrutamientos ni partición o segmentación de paquetes.

También es importante hacer notar que en el nivel capa de transporte no existe control de flujo ni verificación de errores para administrar los paquetes que circula por la red. Sin embargo, algunas implementaciones particulares del TCP/IP como la de Windows si contempla esquemas de verificación de errores.

## CAPA DE APLICACIÓN

Los servicios de aplicación de TCP/IP son idénticos a los de OSI pero incorporan características que en el protocolo de OSI corresponden a las capas de presentación y de sesión. Entre ellos se encuentran los siguientes:

**Telnet**: servicio de terminal remota para permitir a un usuario remoto acceder a los servicios de un servidor como si tuviera conexión directa.

**FTP**: protocolo para transferencia de archivos y servicios de directorio entre terminales remotas.

**SMTP**: protocolo para correo electrónico.

**Kerberos**: protocolo que ofrece servicios de encriptación y codificación de información y otros esquemas de seguridad para aplicaciones de usuario.

**TNS**: este protocolo permite mapear las direcciones lógicas de una terminal a un nombre simbólico más fácilmente identificable pro los usuarios de la red. Ese servicio a su vez es utilizado por otros servicios como el de correo electrónico y FTP.

Todos estos servicios están basados en TCP a nivel capa de transporte y aunque son más simples se usar no son tan seguros, entre ellos están:

**RCP**: éste protocolo se utiliza para que los programas de usuario estén accesibles a otros usuarios en la red ofreciendo a estos últimos una interfaz con el primero.

**TFTP**: idéntico a ftp pero sin verificación de errores.

**SNMP**: Servicio orientado a los administradores de red que permite monitorear a las terminales en red, a los usuarios, a los servicios y finalmente a los recursos existentes en la red.

## DIRECCIONES IP

Las direcciones IP hacen que el envió de datos entre ordenadores se haga de forma eficaz, de un modo similar al que se utilizan los números de teléfono.
Las direcciones IP tienen 32 bits, formados por cuatro campos de 8 bits separados por puntos. Cada campo puede tener un valor comprendido entre 0 y 255. Esta compuesta por una dirección de red, seguida de una dirección de subred y de una dirección de host.

Existen cinco clases de subredes, tal y como muestra a continuación

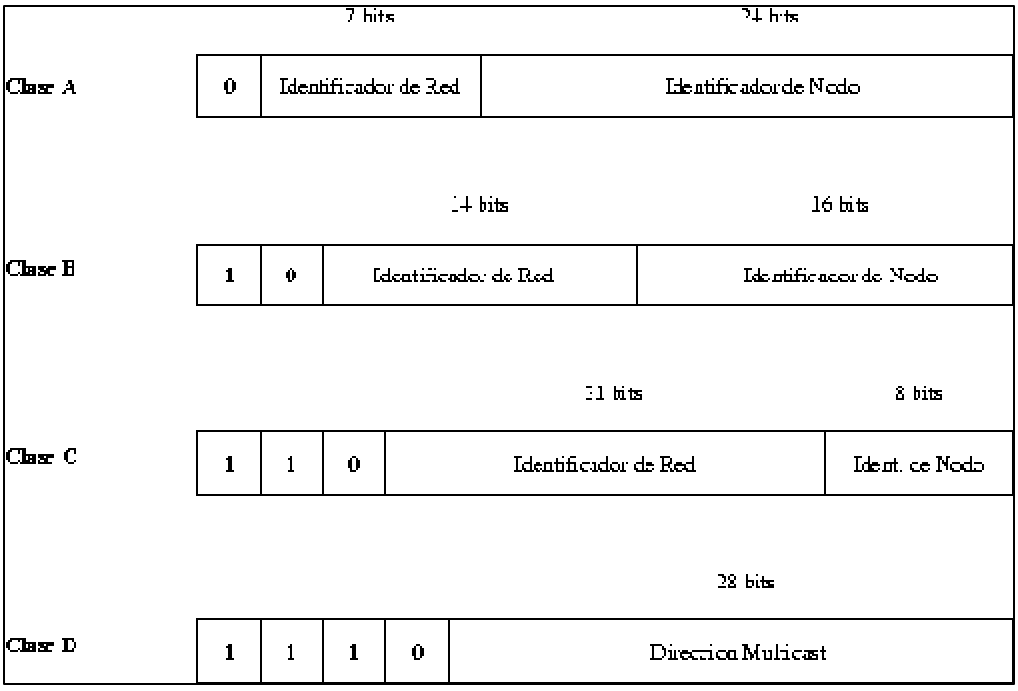



FIGURA D - 2. CLASES DE SUBREDES

- La clase A contiene 7 bits para direcciones de red, con lo que permite tener hasta 128 redes, con 16.777.216 ordenadores cada una. Las direcciones estarán comprendidas entre 0.0.0.0. y 127.255.255.255., y la mascara de subred será 255.0.0.0.
- La clase B contiene 14 bits para direcciones de red y 16 bits para direcciones de hosts. El número máximo de redes es 16.536 redes, con 65.536 ordenadores por red. Las direcciones estarán comprendidas entre 128.0.0.0. y 191.255.255.255., y la mascara de subred será 255.255.0.0.
- La clase C contiene 21 bits para direcciones de red y 8 para hosts, lo que permite tener un total de 2.097.142 redes, cada una de ellas con 256 ordenadores. Las direcciones estarán comprendidas entre 192.0.0.0. y 223.255.255.255., y la mascara de subred será 255.255.255.0.
- La clase D se reserva todas las direcciones para multidestino (multicast), es decir, un ordenador transmite un mensaje a un grupo especifico de ordenadores de esta clase. Las direcciones estarán comprendidas entre 224.0.0.0. y 239.255.255.255.
- La clase E se utiliza exclusivamente para fines experimentales. Las direcciones están comprendidas entre 240.0.0.0. y 247.255.255.255.

## SUBREDES

Debido al crecimiento explosivo de Internet, el uso de direcciones IP asignadas se volvió demasiado rígido para permitir cambiar con facilidad la configuración de redes locales. Estos cambios podían ser necesarios cuando:

- Se instala una nueva red física.
- El crecimiento del número de hosts requiere dividir la red local en dos o más redes.

Para evitar tener que solicitar direcciones IP adicionales en estos casos, se introdujo el concepto de subred.

El número de host de la dirección IP se subdivide de nuevo en un número de red y uno de host. Esta segunda red se denomina *subred*. La red principal consiste ahora en un conjunto de subredes y la dirección IP se interpreta como: número de red.número de subred.número de host

La combinación del número de subred y del host suele denominarse "dirección local" o parte local". La creación de subredes se implementa de forma que es transparente a redes remotas. Un host dentro de una red con subredes es consciente de la existencia de estas, pero un host de un red distinta no lo es; sigue considerando la parte local de la dirección IP como un número de host.

La división de la parte local de la dirección IP en números de subred y de host queda a libre elección del administrador local; cualquier serie de bits de la parte local se puede tomar para la subred requerida. La división se efectúa empleando una *máscara de subred* que es un número de 32 bits. Los bits a cero en esta máscara indican posiciones de bits correspondientes al número de host, y los que están a uno, posiciones de bits correspondientes al número de subred. Las posiciones de la máscara pertenecientes al número de red se ponen a uno pero no se usan. Al igual que las direcciones IP, las máscaras de red suelen expresarse en formato decimal.

El tratamiento especial de "todos los bits a cero" y "todos los bits a uno" se aplica a cada una de las tres partes de dirección IP con subredes del mismo modo que a una dirección IP que no las tiene. Ver Direcciones IP especiales. Por ejemplo, una red de clase B con subredes, que tiene un parte local de 16 bits, podría hacer uso de uno de los siguientes esquemas:

- El primer byte es el número de subred, el segundo el de host. Esto proporciona 254(256 menos dos, al estar los valores 0 y 255 reservados) posibles subredes, de 254 hosts cada una. La máscara de subred es 255.255.255.0.

- Los primeros 12 bits se usan para el número de subred, y los 4 últimos para el de host. Esto proporciona 4094 posibles subredes(4096 menos 2), pero sólo 14 host por subred. La máscara de subred es 255.25.255.240. Hay muchas otras posibilidades.

Mientras el administrados es totalmente libre de asignar la parte de subred a la dirección local de cualquier forma legal, el objetivo es asignar un *número* de bits al número de subred y el resto a la dirección local. Por tanto, es corriente usar un bloque de bits contiguos al comienzo de la parte local para el número de subred ya que así las direcciones son más legibles(esto es particularmente cierto cuando la subred ocupa 8 o 16 bits). Con este enfoque, cualquiera de las máscaras anteriores es buena, pero no máscaras como 255.255.252.252 o 255.255.255.15.

## TIPOS DE "SUBNETTING"

Hay dos tipos de "subnetting": estático y de longitud variable. El de longitud variable es el más flexible de los dos. El tipo de "subnetting" disponible depende del protocolo de encaminamiento en uso; el IP nativo sólo soporta "subnetting" estático, al igual que el ampliamente utilizado RIP. Sin embargo, la versión 2 del protocolo RIP soporta además "subnetting" de longitud variable. Para ver una descripción de RIP y RIP2, ir a RIP("Routing Information Protocol"). Protocolos de encaminamiento analiza los protocolos de encaminamiento en detalle.

### "Subnetting" estático

El "subnetting" estático consiste en que todas las subredes de la red dividida empleen la misma máscara de red. Esto es simple de implementar y de fácil mantenimiento, pero implica el desperdicio de direcciones para redes pequeñas. Por ejemplo, una red de cuatro hosts que use una máscara de subred de 255.255.255.0 desperdicia 250 direcciones IP. Además, hace más difícil reorganizar la red con una máscara nueva. Hoy en día, casi todos los hosts y "routers" soportan "subnetting" estático.

### "Subnetting" de longitud variable

Cuando se utiliza "subnetting" de longitud variable, las subredes que constituyen la red pueden hacer uso de diferentes máscaras de subred. Una subred pequeña con sólo unos pocos hosts necesita una máscara que permita acomodar sólo a esos hosts. Una subred con muchos puede requerir una máscara distinta para direccionar esa elevada cantidad de hosts. La posibilidad de asignar máscaras de subred de acuerdo a las necesidades individuales de cada subred ayuda a conservar las direcciones de red. Además, una subred se puede dividir en dos añadiendo un bit a la máscara. El resto de las subredes no se verán afectadas por el cambio. No todos los hosts y "routers" soportan "subnetting" de longitud variable.
Sólo se dispondrán redes del tamaño requerido y los problemas de encaminamiento se resolverán aislando las redes que soporten "subnetting" de longitud variable. Un host que no soporte este tipo de "subnetting" debería disponer de una ruta de encaminamiento a un "router" que sí lo haga.

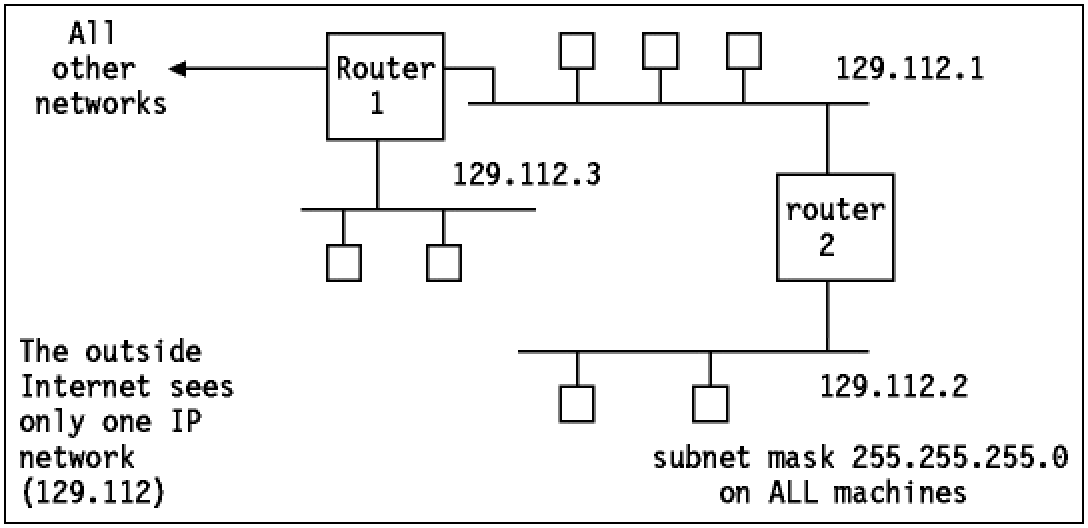
### Mezclando "subnetting" estático y de longitud variable

A primera vista, parece que la presencia de un host que sólo puede manejar "subnetting" estático impediría utilizar "subnetting" de longitud variable en cualquier punto de la red. Afortunadamente no es este el caso. Siempre que los "routers" entre las subredes que tengan distintas máscaras usen "subnetting" de longitud variable, los protocolos de encaminamiento son capaces de ocultar la diferencia entre máscaras de subred a cada host de una subred. Los hosts pueden seguir usando encaminamiento IP básico y desentenderse de las complejidades del "subnetting", que quedan a cargo de "routers" dedicados a tal efecto.

**EJEMPLO DE "SUBNETTING" ESTÁTICO**

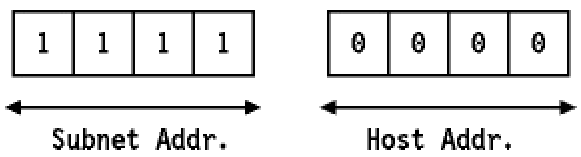
Asumamos que a nuestra red se le ha asignado el número de red IP de clase B 129.112. Tenemos que implementar múltiples redes físicas en nuestra red, y algunos de los "routers" que usaremos no admiten "subnetting" de longitud variable. Por tanto tendremos que elegir una máscara de subred para la totalidad de la red. Tenemos una dirección local de 16 bits para la red y debemos dividirla correctamente en dos partes. Por el momento, no preveremos tener más de 254 redes físicas, ni más de 254 hosts por red, de tal forma que una máscara de subred aceptable sería 255.255.255.0(que además tiene la ventaja de ser legible). Esta decisión debe tomarse cuidadosamente, ya que será difícil cambiarla posteriormente. Si el número de redes o de hosts crece por encima de nuestras previsiones, puede que tengamos que implementar "subnetting" de longitud variable para usar al máximo las 65534 direcciones locales de las que disponemos.

Figura D-3. Una configuración de subred muestra un ejemplo de implementación con tres subredes.




***Configuración de subred*** - Tres redes físicas forman una sola red IP. Los dos "routers" realizan tareas ligeramente diferentes. El "router" 1 actúa como "router" entre las subredes 1 y 3 así como para toda nuestra red y el resto de Internet. El "router" 2 actúa sólo como "router" entre las redes 1 y 2.

Consideremos ahora una máscara de subred diferente: 255.255.255.240. El cuarto octeto se ha dividido por tanto en dos partes:



La siguiente tabla contiene las posibles subredes que usarían esta máscara:

| Hexadecimal value | Subnet number |
|---|---|
| 0000 | 0 |
| 0001 | 16 |
| 0010 | 32 |
| 0011 | 48 |
| 0100 | 64 |
| 0101 | 80 |
| 0110 | 96 |
| 0111 | 112 |
| 1000 | 128 |
| 1001 | 144 |
| 1010 | 160 |
| 1011 | 176 |
| 1100 | 192 |
| 1101 | 208 |
| 1110 | 224 |
| 1111 | 240 |

FIGURA D-4. VALORES DE SUBREDES PARA LA MÁSCARA DE SUBRED 255.255.255.240

Para cada uno de estos valores de subred, sólo 14 direcciones( de la 1 a la 14) de hosts están disponibles, ya que sólo la parte derecha del octeto se puede usar y porque las direcciones 0 y 15 tienen un significado especial tal como se describe en Direcciones IP especiales.

De este modo, el número de subred 9.67.32.16 contendrá a los hosts cuyas direcciones IP estén en el rango de 9.67.32.17 a 9.67.32.30, y el número de subred 9.67.32.32 a los hosts cuyas direcciones IP estén en el rango de 9.67.32.33 a 9.67.32.46, etc.

## PUERTOS Y PROTOCOLOS TCP/UDP

Cada proceso que se desea comunicar con otro se identifica en la pila de protocolos TCP/IP con uno o más puertos. Un puerto es un número de 16 bits, empleado por un protocolo host - a - host para identificar a que protocolo del nivel superior o programa de aplicación se deben entregar los mensajes recibidos.

### TCP

El protocolo TCP proporciona un servicio de comunicación que forma un circuito, es decir, que el flujo de datos entre el origen y el destino parece que sea continuo. TCP proporciona un circuito virtual el cual es llamado una conexión.

Al contrario que los programas que utilizan UDP, los que utilizan el TCP tienen un servicio de conexión entre los programas llamados y los que llaman, chequeo de errores, control de flujo y capacidad de interrupción.

### UDP

El protocolo UDP (User Datagram Protocol) proporciona aplicaciones con un tipo de servicio de datagramas orientado a transacciones. El servicio es muy parecido al **protocolo IP** en el sentido de que no es fiable y no esta orientado a la conexión. El UDP es simple, eficiente e ideal para aplicaciones como el TFTP y el DNS. Una dirección IP sirve para dirigir el datagrama hacia una maquina en particular, y el número de puerto de destino en la cabecera UDP se utiliza para dirigir el datagrama UDP a un proceso especifico localizado en la cabecera IP. La cabecera UDP también contiene un número de puerto origen que permite al proceso recibido conocer como responder al datagrama.

En la siguiente Tabla D-1 se muestran algunos de los puertos (existen $2^{16}$=65,536) con sus respectivos protocolos y la descripción del servicio al que están asignados:

| Puerto | Protocolo | Servicio |
|---|---|---|
| 7 | UDP | Echo |
| 18 | TCP | Message Send |
| 21 | TCP, UDP | FTP File Transfer |
| 23 | TCP | Telnet |
| 25 | TCP | SMTP Outgoing mail |
| 69 | TCP, UDP | TFTP (Trivial File Transfer) |
| 80 | HTTP | World Wide Web |
| 88 | TCP | Kerberos |
| 101 | TCP | Hostnames |
| 110 | TCP | POP incoming mail |
| 113 | TCP | Auth (Authentication Service) |
| 118 | TCP | SQL Services |
| 139 | TCP, UDP | NETBIOS Session Service |
| 156 | TCP | SQL Service |
| 280 | TCP | HTTP Management |
| 443 | TCP | HTTP over SSL |
| 465 | TCP | SMTP over SSL |
| 5050 | TCP | Yahoo Messanger |
| 54321 | UDP | Back Orifice 2000 (UDP) |

# ANEXO E

## CRIPTOGRAFÍA

La palabra criptografía proviene de las raíces griegas *kryptos* (ocultar) y *graphos* (escribir), por lo que literalmente significa esconder escritura. En la práctica, es el arte y la ciencia de ocultar información.

Consiste de un conjunto de técnicas o procedimientos que alteran los símbolos que utilizamos para comunicarnos, pero sin variar su contenido, con el fin de convertir la información en un conjunto de signos sin valor para quienes no tienen la clave, llave o fórmula para descifrarlos.

Su gran utilidad para el manejo de información confidencial ha impulsado su constante estudio y evolución. En sus inicios la criptografía fue utilizada con fines militares. Fue así que desde el siglo VI A.C., en la antigua Grecia, ya se utilizaban algunas técnicas criptográficas con este propósito. También desde entonces surgió el criptoanálisis o estudio de métodos para descifrar o descodificar el texto cifrado y recuperar el texto original. Comenzó la escalada para crear técnicas o procedimientos cada vez más sofisticados tanto para encriptar como para desencriptar.

### CRIPTOGRAFÍA ESTRATÉGICA

Actualmente su aplicación se ha extendido a diversas actividades basadas en el uso de la tecnología de la información y las comunicaciones (TIC) constituyéndose en un elemento indispensable para garantizar la seguridad en el manejo de la información. Estas herramientas han permitido proteger cada carácter con una llave que puede conformarse hasta por 256 bits. Es decir, que para encontrar esta llave en particular, tendríamos que buscarla entre $1.15 \times 10^{77}$ combinaciones posibles.

Recuerde que $1.15 \times 10^{77}$ equivale a:
1150000000000000000000000000000000000000000000000000000000000000000000000000000000000000

La computadora más rápida y moderna, se tardaría $1.83 \times 10^{60}$ años de trabajo para obtener dichas combinaciones.

Recuerde que $1.83 \times 10^{60}$ equivale a:

1830000000000000000000000000000000000000000000000000000000000000000000000000

*Claro que hay la posibilidad de encontrar la llave al explorar las primeras combinaciones, sin embargo es muy remota.*

En resumen, ya sea por su uso militar o por su uso en aplicaciones comerciales, la criptografía es un factor de desarrollo estratégico para todos los países.

## MÉTODOS CRIPTOGRÁFICOS

En general, existen dos métodos empleados para encriptar texto, video, sonido, gráficos o software, de manera que pueda ser recuperada por una persona que conozca la clave apropiada.

### 1.- CIFRADO SIMÉTRICO

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que es un criptosistema *simétrico*. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. Se pueden dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y cifradores en flujo, que trabajan sobre flujos continuos de bits.

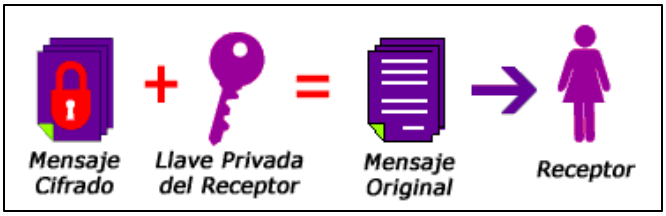
Éstos sistemas son también conocidos como sistemas de secreto compartido o de clave privada, pero los requerimientos para intercambio de claves los hacen difíciles de usar. Agrupados dentro de esta modalidad, existen métodos elementales llamados clásicos, que se han utilizado desde la antigüedad. Por ejemplo: Sustitución y Transposición.

DES and AES-Rijndael son cifradores simétricos.

### 2.- CIFRADO ASIMÉTRICO

Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es *asimétrico* o de clave pública. Una clave, *la privada*, se mantiene secreta y se utiliza para cifrar. Mientras que la segunda clave, *la pública*, puede ser conocida por todos y se usa para decifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales (Ver Glosario).


PARA TRANSMITIR UN MENSAJE, EL EMISOR ENCRIPTA EL TEXTO CON LA LLAVE PÚBLICA DEL RECEPTOR.




EL RECEPTOR DEL MENSAJE LO DESENCRIPTA CON SU LLAVE PRIVADA (QUE SÓLO ÉL CONOCE) ELIMINANDO ASÍ EL INTERCAMBIO DE LLAVES.

Este método es el principio de la firma digital y actualmente garantiza la seguridad en el manejo de información en medios electrónicos, así como su integridad y autenticidad.

Debido a que los cifradores asimétricos tienden a ser mas intensos computacionalmente, son usualmente utilizados en combinación con cifradores simétricos para implementar criptografía de llave pública. El cifrador asimétrico es utilizado para encriptar una llave de sesión y la llave encriptada de sesión es usada para encriptar el mensaje actual. Esto brinda los beneficios del intercambio de llaves de los cifradores asimétricos con la velocidad de cifradores simétricos.

Existen varias técnicas de llave pública: RSA, Diffie-Hallman,Rabin, ElGamal, Mc Eliece, Knapsack, entre otros, siendo la primera las más conocida y utilizada mundialmente.

# ANEXO F - HERRAMIENTAS PARA DETECCIÓN Y ACCESO A WLANS

| HERRAMIENTA / WEBSITE | DESCRIPCIÓN |
|---|---|
| NetStumbler www.netstumbler.com | Identificador de puntos de acceso inalámbricos. Gratuito. |
| Kismet www.kismetwireless.net | Escudriña y monitorea redes inalámbricas. Identifica SSID, MAC's, canales y velocidades de conexión. Gratuito. |
| THC-RUT www.thehackerschoice.com | Descubre redes inalámbricas. Usa "fuerza bruta". Gratuito. |
| Ethereal www.ethereal.com | Analizador interactivo de tráfico de redes inalámbricas. Gratuito. |
| AirSnort airsnort.shmoo.com | Calcula y rompe la llave de encripción. Monitoreo pasivo. Gratuito. |
| HostAP hostap.epitest.fi | Convierte computadora en un Punto de Acceso. |
| WEPWedgie sourceforge.net projects /wepwedgie | Rompe WEP. Escanea puertos. Inyecta tráfico. Lógica para reglas firewall. |
| WEPCrack sourceforge.net/projects /wepcrack | Rompe WEP bajo algoritmo RC4. Gratuito. |
| AirSnarf airsnarf.shmoo.com/ | Roba passwords y nombres de usuario. Redirección de DNS y Http usando otro punto de acceso. |
| SMAC www.klcconsulting.net/smac | Permite cambiar direcciones MAC bajo sistemas Windows. |
| Airjack sourceforge.net /projects/airjack | Herramienta de ataque: Negación de Servicio (DoS), tira todas las conexiones. |
| IRPAS ww.phenoelit.de/irpas/ | Ataca protocolo de ruteo de Internet: CDP, DHCP, IGRP y HSRP. |
| Ettercap ettercap.sourceforge.net | Analiza y filtra tráfico al vuelo. Usa ataque de intercepción / inserción. |
| Cain&Abel www.oxid.it | Recupera y decodifica passwords vía ataques de diccionario, fuerza bruta y análisis criptográfico. Analiza protocolos de ruteo. |
| Hotspotter www.remote-exploit.org/codes.html | Punto de Acceso falso. Pasivo. Identifica redes de los clientes. |
| WEP Attack sourceforge.net/projects/wep attack/ | Rompe WEP usando ataques de Fuerza Bruta y de Diccionario. |
| ASLEAP asleap.sourceforge.net | Recupera passwords y re-autentica usuarios bajo redes LEAP, escudriñador. |
| THC-LeapCracker www.thc.org | Rompe protocolo LEAP de autenticación de CISCO. Ataques de diccionario. |
| DSNIFF naughty.monkey.org /~dugsong/dsniff | Auditoria de red, pruebas de penetración y monitoreo pasivo de red. Ataque de intercepción / inserción. |
| IKEcrack ikecrack.sourcefoge.net/ | Ataques: Fuerza Bruta y Diccionario bajo autenticación PSK-IKE. |
| Nessus www.nessus.org | Escudriñador de seguridad remoto. |

# LISTADO DE TABLAS

## CAPITULO I



## CAPITULO II



## CAPITULO III



## CAPITULO IV



## ANEXOS

# LISTADO DE FIGURAS

## CAPITULO I



## CAPITULO II



## CAPITULO III

# Listado de Figuras

## CAPITULO IV



## ANEXOS

# BIBLIOGRAFÍA


1. Intel Centrino Mobile Technology. [en línea] 2005. http://www.intel.com/personal/wireless/index.htm

2. 802.11 standards: 802.11b, 802.11a, 802.11g: Which one is right for you. [en línea] 2006. http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm

3. Seguridad de las redes inalámbricas: Wardriving y Warchalking - Hispasec. [en línea] 2002. http://www.hispasec.com/unaaldia/1486

4. Dennis Fisher. *Study Exposes WLAN Security Risks*. [en línea] 2003. http://www.eweek.com/print_article/0,3048,a=38444,00.asp

5. Rob Flickenger. *Antenna on the Cheap(er, Chip)*. [en línea] 2001. http://www.oreillynet.com/pub/wlg/448

6. *AirJack.* [en línea]. 2005 *http://www.wirelessve.org/entries/show/WVE-2005-0018*

7. *Wellenreiter* - WLAN Hacking. [en línea] 2005. http://www.wellenreiter.net/

8. *WEPCrack Project Info* [en línea]. *2004.* http://sourceforge.net/projects/wepcrack

9. *AirSnort Homepage* [en línea]. 2005. http://airsnort.shmoo.com/

10. *Authentication and Privacy*. En ANSI / IEEE Standard 802.11. [en línea]. 1999. http://standards.ieee.org/getieee802/download/802.11-1999.pdf , 59-68 pp.

11. Suhdir Nath. *802.1x Overview.* [en línea]. 2003. http://www.cisco.com/warp/public/732/Tech/security/docs/8021xoverview.ppt

12. Paul Congdon. *IEEE 802.1x Overview Port Based Network Access Control.* [en línea]. 2000. http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF

13. IEC. *EAP Methods for 802.11. Wireless LAN Security*. [en línea]. 2005. http://www.iec.org/online/tutorials/acrobat/eap_methods.pdf

14. Wi-Fi Alliance. *Overview: Wi-Fi Protected Access 2*. [en línea]. 2002. http://www.wi-fi.org/OpenSection/protected_access.asp

15. *WPA's Little Secret*. [en línea]. 2003. http://www.stargeek.com/item/20270.html

17. Nikita Borisov, Ian Goldberg, David Wagner. [en línea]. 2001. *Security of the WEP algorithm*. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

# BIBLIOGRAFÍA


1. Stewart, M., *Seguridad en WiFi*, Mc Graw Hill, México, 2003.

2. Reid y Seide, *802.11 (Wi-Fi) Manual de Redes Inalámbricas*, Mc Graw Hill, México, 2003.

3. Rivera, R., *Redes Locales Inalámbricas*, UNAM – Campus Acatlán, México, 2003.

4. 802.11 standards: 802.11b, 802.11a, 802.11g: Which one is right for you? [en línea]. [Disponible en] http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm [Consulta: 12 Marzo 2001]

5. Authentication and Privacy [en línea]. En ANSI / IEEE Standard 802.11, 1999 Edition. [Disponible en] http://standards.ieee.org/getieee802/download/802.11-1999.pdf , 59-68 pp.

6. Muller, N., *Wi-Fi for the Enterprise*, Mc Graw Hill, U.S.A., 2004.

7. Roeder, K., *Wi-Fi Handbook*, Mc Graw Hill, U.S.A., 2004.

8. LaRocca y LaRocca, *802.11 Demystified*, McGraw-Hill, U.S.A., 2004.

9. Klander, L., *Hacker Proof The Ultimate Guide to Network Security,* Jamsa Press, U.S.A., 2001.

10. Scott, et al., *Virtual Private Networks*, O´Reilly, U.S.A., 1999.

11. Lepage y Iarrera, *UNIX System Administrator's Bible*, IDG Books, U.S.A., 1989.

12. Scambray et al., *Hacking Exposed,* Osborne/McGraw-Hill, U.S.A., 2001.

13. Hunt, C., *TCP/IP Network Administration,* O´Reilly & Assosiates, Inc., U.S.A., 1994.

14. Stevens, R., *TCP/IP Illustrated: The Protocols Volume I*, Addison-Wesley Publishing Company, U.S.A., 1994.

# GLOSARIO

## A

Ad Hoc
Una WLAN bajo topología "Ad Hoc" consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones "Ad Hoc" son comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal y SSID en modo "Ad Hoc".

AES - Estándar de Cifrado Avanzado (Advanced Encryption Standard)
También conocido como "Rijndael", algoritmo de encriptación simétrica de 128 bit desarrollado por los belgas Joan Daemen y Vincent Rijmen. En Octubre de 2000 era seleccionado, gracias a su buena combinación de seguridad, velocidad, eficiencia, sencillez y flexibilidad, por el Instituto Nacional de Estándares y Tecnología (NIST) norteamericano como estándar de cifrado reemplazando al hasta entonces estándar DES.
Con su algoritmo los autores vencieron a criptólogos de considerable fama mundial y a empresas de renombre como IBM, RSA y Counterpane.

Ancho de Banda
El es el rango de frecuencias en el que una señal determinada existe.
Para señales analógicas, el ancho de banda es la anchura, medida en hercios, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. Puede ser calculado a partir de una señal temporal mediante el análisis de Fourier. También son llamadas frecuencias efectivas las pertenecientes a este rango.
La frecuencia es la magnitud física que mide las veces por unidad de tiempo en que se repite un ciclo de una señal periódica. Una señal periódica de una sola frecuencia tiene un ancho de banda mínimo. En general, si la señal periódica tiene componentes en varias frecuencias, su ancho de banda es mayor, y su variación temporal depende de sus componentes frecuenciales.
Normalmente las señales generadas en los sistemas electrónicos, ya sean datos informáticos, voz, señales de televisión, etc. son señales que varían en el tiempo y no son periódicas, pero se pueden caracterizar como la suma de muchas señales periódicas de diferentes frecuencias.

Antena
Dispositivo generalmente metálico capaz de radiar y recibir ondas de radio que adapta la entrada/salida del receptor/transmisor del medio. Dependiendo de hacia que punto emitan la señal podemos encontrarlas direccionales u omnidireccionales

Appliance Server
Servidores dedicados a distribuir y compartir Internet, servicios FTP, e-mail, conexiones VPN, servicios de cortafuegos (firewall), de impresora y archivo y también operan como servidores web que incorporan hardware y software en el mismo producto de modo que todas las aplicaciones se encuentran preinstaladas. El servidor está conectado dentro de una red existente y puede comenzar a funcionar casi de inmediato con una mínima configuración y mantenimiento.

AP - Access Point
Punto de acceso, estación base de una red Wi-Fi que conecta clientes inalámbricos entre sí y a redes de cable.

Arp
El protocolo Address Resolution Protocol (ARP - RFC826) es usado para traducir una dirección IP de 32-bits a una dirección Ethernet de 48-bits.Para ilustrarlo, cuando un host A (192.168.1.1) quiere comunicarse con un host B (192.168.1.2), la dirección IP conocida debe ser traducida a una dirección MAC utilizando el protocolo ARP. Para hacerlo, el host A envía un mensaje de diseminación extensa (broadcast) conteniendo la dirección IP del host B (¿Quién tiene 192.168.1.2? Decírselo a 192.168.1.1). El host objetivo, reconociendo que la dirección IP en los paquetes coincide con la suya propia, devuelve una respuesta (192.168.1.2 está en 01:23:45:67:89:0A). La respuesta es típicamente almacenada en la caché.

## B

Bluetooth
Estándar de comunicación inalámbrica que utiliza FHSS, capaz de transmitir a velocidades de 1 Mbps a una distancia de 10 metros entre aparatos (normalmente portátiles, impresoras, monitores, teclados, ratones, etc....) que implementen esta tecnología ya que su FHSS/Hopping Pattern es de 1600 veces por segundo, lo que asegura transmisiones altamente seguras. En cuanto a su implementación Bluetooth utiliza el término piconet . Un piconet es un grupo de 2 u 8 aparatos que utilizan "Bluetooth" que comparten el mismo rango que es utilizado por un "Hopping Sequence", a su vez cada piconet contiene un aparato principal ("master") que es el encargado de coordinar el "Hopping Pattern" del piconet para que los demás aparatos ("slaves") sean capaces de recibir información.

Bridge (Puente)
Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar

Broadcast - Transmitir, diseminar ó comunicar extensamente. Transmisión de uso público.

BSSID **-** Basic Service Set Identifier, Dirección MAC del punto de acceso.

## C

CCMP
Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol, protocolo de encriptación utilizado en WPA2, basado en la suite de cifrado de bloques AES.

Centrino
Tecnología móvil desarrollada por Intel compuesta por un procesador Pentium M, chipset 855 y conectividad inalámbrica integrada.

Certificado Digital
Es la certificación electrónica que emiten las Autoridades Certificadoras donde constan unos datos de verificación de firma a un signatario y confirma su identidad. Entre los datos figuran la fecha de emisión y la fecha de caducidad, la clave pública y la firma digital del emisor. Los Certificados Digitales siguen las estipulaciones del estándar X.509. Este documento sirve para vincular una clave pública a una entidad o persona.

CHAP - Challenge Handshake Authentication Protocol
Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, mucho más seguro que el PAP. Una vez efectuado el enlace, el servidor envía un mensaje de desafío al solicitante de la conexión, el cual responde con un valor hash que será comparado por el servidor con sus cálculos del valor hash esperado. Si el valor coincide, la autenticación prospera, de lo contrario, finaliza. En cualquier momento el servidor puede solicitar un mensaje de desafío. Debido a que los identificadores cambian frecuentemente y por que la autenticación puede ser solicitada en cualquier momento.

Cliente Inalámbrico (Wireless Client)
Toda solución suceptible de integrarse en una red wireless como PDAs, portátiles, cámaras inalámbricas, impresoras, etc...

Cracker
Programadores especializados en romper, abrir, buscar una falla o quebrantar sistemas particulares, ya sea para robar datos o dañarlos.

CRC
Cyclic Redundancy Check, pseudo-algoritmo de integridad usado en el protocolo WEP (débil).

## D

DHCP
Protocolo de configuración dinámico para clientes. Utiliza los puertos 67 y 68 vía UDP.
Este protocolo es usado por algunos nodos de red para restablecer su configuración de red en forma automática utilizando un servidor central. Se pueden proveer varios elementos en su configuración como son: el nombre y la IP del DNS; la IP del cliente, la máscara, ruteador por defecto y las IP de los servidores de WINS entre otros muchos.

Diffie-Hellman
Cifrador simétrico definido en la patente numero 4,200,770 de lose u en 1977. Expiro el 6 de Septiembre de 1977.

Dispositivo Móvil (DM)
Ya sea Tarjeta PCMCIA, USB, PCI, Centrino, que sustituyen a las tarjetas de red. Su función es la de recibir/enviar información desde la estación en que están instaladas (portátiles, PDAs, móviles, cámaras, impresoras, etc.)

DSSS - Espectro Amplio mediante Secuencia Directa (Direct Sequence Spread Spectrum)
A diferencia de la técnica de transmisión de Espectro Amplio (Spread Spectrum) FHSS, DSSS no precisa enviar la información a través de varias frecuencias sino mediante transmisores; cada transmisor agrega bits adicionales a los paquetes de información y únicamente el receptor que conoce el algoritmo de estos bits adicionales es capaz de descifrar los datos .Es precisamente el uso de estos bits adicionales lo que permite a DSSS transmitir información a 10Mbps y una distancia máxima entre transmisores de 150 metros. Un estándar que utiliza DSSS es IEEE 802.11b.

## E

EAP - Protocolo de Autenticación Extensible (Extensible Authentication Protocol)
Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros. Junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virutla (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación, como CHAP.

EAPOL
EAP Over LAN, protocolo usado en redes inalámbricas para transportar EAP.

Estándar 802.11
Se refiere a una familia de especificaciones desarrollada por el IEEE y aprobada por ésta en 1997 para tecnologías de red inalámbricas y especifica un interfaz aéreo entre un cliente inalámbrico y una estación base o entre dos clientes wireless. Existen diversas especificaciones aplicadas a las redes inalámbricas dentro de la familia 802.11:

802.11 -- ofrece una velocidad de transmisión de 1 o 2 Mbps en la banda de frecuencia de los 2.4 Ghz empleando bien frequency hopping spread spectrum (FHSS) o direct sequence spread spectrum (DSSS).

802.11a -- ofrece hasta 54 Mbps en la banda de los 5GHz. Emplea un esquema de codificación orthogonal frequency division multiplexing encoding scheme en lugar de FHSS o DSSS.

802.11b (también conocido como 802.11 High Rate o Wi-Fi) -- ofrece hasta 11 Mbps (con un retroceso de 5.5, 2 y 1 Mbps) en la banda de 2.4 GHz con 13 canales disponibles. Emplea sólo DSSS. 802.11b fue ratificado en 1999 lo que permitió una funcionalidad wi-fi comparable a Ethernet.

802.11g --ofrece 20+ Mbps en la banda de 2.4 GHz.

## F

FHSS
Espectro Amplio mediante Saltos de Frecuencia (Frequency Hopping Spread Spectrum)
Primer desarrollo de la técnica de transmisión del Espectro Amplio (Spread Spectrum) que, al igual que Ethernet, divide los datos en paquetes de información pero que, por motivos de seguridad, para dificultar su interceptación por terceros, los envía a través de varias frecuencias (Hopping Pattern) seleccionadas al azar y que no se superponen entre sí. Para llevar acabo la transmisión además es necesario que tanto el aparato emisor como el receptor coordinen este "Hopping Pattern".

Firma Digital
Este mecanismo implica el cifrado, por medio de la clave privada del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se vuelve parte del mensaje a ser enviado. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no rechazo. Esto tiene dos efectos:

- Cualquier cambio al mensaje puede ser detectado, debido al algoritmo del mensaje codificado.
- No puede rehusarse a firmar el mensaje.

Estas dos características, integridad del mensaje y no rechazo, hacen de las firmas digitales un componente muy útil para aplicaciones de comercio electrónico.

Firewall
Equipo de cómputo que filtra y controla el tráfico, entrante o saliente, entre redes a nivel de puertos, sesiones y contenido. Normalmente ubicado en la frontera de la red. Evita que intrusos tengan acceso a información confidencial. Muchas de las amenazas a la perdida de información, como virus, gusanos y ataques combinados explotan vulnerabilidades como puertos abiertos para entrar en las redes.

Los ataques no solo vienen de afuera hacia adentro, y no solo hay que controlar el tráfico entrante. Una vez se ha instalado un programa troyano dentro de su red, este puede enviar grandes cantidades de información hacia afuera (por cualquier puerto) y si su firewall o su administrador de red solo ha bloqueado la entrada de intrusos nunca se dará cuenta que le están sacando información.

Si no cuenta con un firewall su red estará expuesta a cualquier tipo de ataque.

Su función principal es la de brindar seguridad contra intrusos y ataques.

## G

GEK - Group Encryption Key, clave para la encriptación de datos en tráfico multicast (también usada para la integridad en CCMP).

GIK - Group Integrity Key, clave para la encriptación de datos en tráfico multicast (usada in TKIP).

GMK - Group Master Key, clave principal de la jerarquía de group key.

GTK - Group Transient Key, clave derivada de la GMK.

## H

Hacker
En este texto el termino hacker se refiere al intruso contra el cual hay que protegerse, independientemente de sus intenciones, conocimientos y habilidades de cómputo.
Los medios han catalogado a todos los intrusos de sistemas como hackers independientemente de una definición apropiada y aplicable para el individuo que ataca un sistema.

Sin embargo existen algunas definiciones:

- En sus inicios el término fue usado en forma benigna, el MIT o Stanford los describía como programadores brillantes y constructivos quienes iniciaron la revolución en cómputación. Su intención era hacer la tecnología accesible y abierta para todos.
- Hack – cortar, tajar o acuchillar. Cortar en pedazos.
- Alguien quien ilegalmente ingresa en un sistema electrónico para obtener información secreta o robar dinero. Persona que es experto en el uso o programación de computadoras.
- Gente fascinada con la resolución de problemas y creación de soluciones usando la tecnología.

Hash
Un valor hash, también conocido como "message digest", es un número generado a partir de una cadena de texto. El hash es sustancialmente más pequeño que el texto en sí, y es generado por una fórmula de tal forma que sea poco probable que algún otro texto produzca el mismo valor. Los hashes juegan un papel crucial en la seguridad donde se emplean para asegurar que los mensajes transmitidos no han sido manipulados. El emisor genera un hash del mensaje, lo encripta y lo envía con el propio mensaje. El receptor luego decodifica ambos, produce otro hash del mensaje recibido y compara los dos hashes, si coinciden, existe una probabilidad muy elevada de que el mensaje recibido no haya sufrido cambios desde su origen.

## I

IAS
Microsoft incluyó con Windows 2000 Server el servicio de autenticación para Internet (IAS - Internet Autentication service) en el que parte de su funcionalidad implementa el protocolo 802.1X que provee un medio para autenticar dispositivos que se conecten a una red LAN. Este estándar utiliza un servidor central de autenticación (con directorio activo) y valida a los usuarios tanto de la red inalámbrica como la red convencional.

ICV Valor de verificación de Integridad (Integrity Check Value)
Campo de datos unido a los datos de texto para la integridad (basado en el algoritmo débil CRC32).

IEEE
Siglas del "Institute of Electrical and Electronic Engineers" (http://www.ieee.org) formado a fecha de julio de 2003 por 377.000 miembros en 150 países. Cuenta con 900 estándares activos y 700 en desarrollo.

IETF
Siglas de "The Internet Engineering Task Force" (http://www.ietf.org), grupo principal auto-organizado comprometido en el desarrollo de nuevas especificaciones estándares para Internet.

Infraestructura - Infrastructure
Topología de una red inalámbrica que consta de dos elementos básicos: estaciones cliente wireless y puntos de acceso.

IPsec - IP Security
Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, encripta todo.

ISO 17999
Estándar para la gestión de la seguridad de la información.

IV Vector de Inicialización (Initialization Vector)
Datos combinados en la clave de encriptación para producir un flujo de claves único.

**K**

KC - (Key Confirmation Key) clave de integridad que protege los mensajes handshake.

KEK - (Key Encryption Key) clave de confidencialidad que protege los mensajes handshake.

**L**

LDAP - Protocolo de Acceso Ligero a Directorio (Lightweight Directory Access Protocol)
Protocolo para el acceso a directorios jerárquicos de información. Basado en el estándar X.500, pero significativamente más simple por lo que también se le denomina x.500-lite, se diferencia de éste porque soporta TCP/IP, necesario para cualquier tipo de acceso a Internet. Aunque no está ampliamente extendido, debería poderse implementar en la práctica mayoría de aplicaciones que se ejecutan virtualmente sobre plataformas informáticas para obtener información de directorios tales como direcciones de correo y llaves públicas. Ya que es un protocolo abierto, no afecta el tipo de servidor en el que se aloje el directorio.

LEAP
Protocolo del tipo EAP patentado por Cisco basado en nombre de usuario y contraseña que se envía sin protección.

**M**

MAC - Control de Acceso al Medio
Dirección hardware que identifica únicamente cada nodo de una red. En redes IEEE 802, la capa Data Link Control (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: Logical Link Control (LLC) y Media Access Control (MAC), la cual se conecta directamente con el medio de red. Consecuentemente, cada tipo de medio de red diferente requiere una capa MAC diferente. En redes que no siguen los estándares IEEE 802 pero sí el modelo OSI , la dirección del nodo se denomina Control de Enlace de Datos (DLC - Data Link Control).

Mbps (Megabits por segundo)
Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.

MD5
Algoritmo de encriptación de 128-bits del tipo EAP creado en 1991 por el profesor Ronald Rivest para RSA Data Security, Inc. empleado para crear firmas digitales. Emplea funciones hash unidireccionales, es decir, que toma un mensaje y lo convierte en una cadena fija de dígitos. Cuando se utiliza una función hash de una dirección, se puede comparar un valor hash frente a otro que esté decodificado con una llave pública para verificar la integridad del mensaje. Basado en Nombre de Usuario y Contraseña, EL PRIMERO SE ENVÍA sin protección. Sólo autentica el cliente frente al servidor, no el servidor frente al cliente.

MHz (Megahertzio)
Unidad empleada para medir la "velocidad bruta" de los microprocesadores equivalente a un millón de hertzios.

MIC - Código de Integridad de Mensajes (Message Integrity Code)
Campo de datos unido a los datos de texto para la integridad (basado en el algoritmo Michael).

MK - (Master Key)
Clave principal conocida por el suplicante y el autenticador tras el proceso de autenticación 802.1x.

MPDU - (Mac Protocol Data Unit)
Paquete de datos antes de la fragmentación.

MS-CHAP - Protocolo de Autenticación por Desafío Mutuo (Challenge Handshake Authentication Protocol)
Protocolo de autenticación utilizado por el acceso remoto de Microsoft y conexiones de red y de acceso telefónico. Con CHAP los clientes de acceso remoto pueden enviar de forma segura sus credenciales de autenticación a un servidor de acceso remoto. Microsoft ha creado una variante de CHAP específica de Windows denominada MS-CHAP. Challenge Handshake Authentication Protocol se llama también CHAP.

MSDU
Mac Service Data Unit, paquete de datos después de la fragmentación.

**N**

NIC
Tarjeta de Red o Network Interface Card. Sirve para comunicarse a la red con otros dispositivos.

**O**

OFDM - Orthogonal Frequency Division Multiplexing
Técnica de modulación FDM (empleada por el 802.11a wi-fi) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal.

**P**

PAE
Port Access Entity, puerto lógico 802.1x.

PAP - Protocolo de Autenticación de Claves (Password Authentication Protocol)
El método más básico de autenticación, en el cual el nombre de usuario y la contraseña (clave) se transmiten a través de una red y se compara con una tabla de parejas nombre-clave. Típicamente, las contraseñas almacenadas en la tabla se encuentran encriptadas. El principal defecto de PAP es que tanto el nombre de usuario como la clave se transmiten sin codificar, a diferencia de sistema CHAP.

PEAP - Protected Extensible Authentication Protocol
Protocolo del tipo EAP desarrollado conjuntamente por Microsoft RSA Security y Cisto para la transmisión datos autenticados, incluso claves, sobre redes inalámbricas 802.11. Autentica clientes de red wi-fi empleando sólo certificados del lado servidor creando un túnel SSL/TLS encriptado entre el cliente y el servidor de autenticación. El túnel luego protege el resto de intercambios de autenticación de usuario.

Phishing
Técnica en auge que consiste en atraer mediante engaños a un usuario hacia un sitio web fraudulento donde se le insta a introducir datos privados, generalmente números de tarjetas de crédito, nombres y passwords de las cuentas, números de seguridad social, etc. Uno de los métodos más comunes para hacer llegar a la "víctima" a la página falsa es a través de un e-mail que aparenta provenir de un emisor de confianza (banco, entidad financiera u otro) en el que se introduce un enlace a una web en la que el "phiser" ha reemplazado en la barra de dirección del navegador la verdadera URL para que parezca una legal.
Una de las consecuencias más peligrosas de este fraude es que la barra "falsa" queda en memoria aún después de salir de la misma pudiendo hacer un seguimiento de todos los sitios que visitamos

posteriormente y también el atacante puede observar todo lo que se envía y recibe a través del navegador hasta que éste sea cerrado.
Una manera para el usuario de descubrir el engaño es que no se muestra la imagen del candado en la parte inferior del navegador que indica que la navegación es segura.

Portadora
Es la onda electromagnética empleada en telecomunicaciones para la transmisión de señales. Se utiliza como base para modificarla (modularla) según la información del emisor. Debe tener una frecuencia de al menos el doble de la frecuencia de la señal original y típicamente es mucho mayor que la de ésta última.
Esta onda portadora es de una frecuencia mucho más alta que la de la señal moduladora (la señal que contiene la información a transmitir).
La razón por la cual se emplea este método de transmitir información es porque es más fácil transmitir una señal de frecuencia alta y el alcance es mayor.
En comunicaciones de radio por ejemplo la longitud de onda de la señal sigue la relación longitud de onda (en metros) = 300 / frecuencia (en megahercios).
Así por ejemplo para transmitir una señal de 20 Khz (que tendría de longitud de onda 15 Km) necesitaríamos una antena de varios kilómetros. Modulando dicha señal podremos disminuir el tamaño de la antena necesaria.
Las ondas portadoras son usadas cuando se transmiten señales de radio a un radiorreceptor. Tanto las señales de modulación de amplitud (AM) como las de frecuencia modulada (FM) son transmitidas con la ayuda de frecuencias portadoras. La frecuencia para una estación de radio dada es en realidad la frecuencia de su onda portadora.

PMK - Par de llaves Maestras (Pairwise Master Key)
Clave principal de la jerarquía de pares de llaves.

PKI - Infraestructura de Clave Pública (Public Key Infrastructure )
Sistema de certificados digitales, Autoridades Certificadores y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet. Los estándares de PKI siguen evolucionando, aunque se estén implementando de forma generalizada como elemento necesario del comercio electrónico. La infraestructura de claves públicas se llama también PKI.

Punto de Acceso (PA) - Access Point (AP)
Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

PSK
Pre-Shared Key, clave derivada de una frase de acceso que sustituye a la PMK normalmente enviada por un servidor de autenticación.

PTK - Par de llaves pasajeras (Pairwise Transient Key)
Clave derivada de la PMK.

**R**

RADIUS - Remote Authentication Dial-In User Service
Servicio de autenticación de usuarios remotos , vía telefónica. Empleado por la mayoría de proveedores de servicios de Internet (ISPs) no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que verificará que la información es correcta y autorizará el acceso al sistema del ISP si es así.

RAS - Servidor de Acceso Remoto (Remote Access Server)
Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta. Permite a los usuarios, una vez autenticados, obtener acceso a los archivos y servicios de impresora de una LAN desde una localización remota.

RC4
Es un algoritmo cifrador de flujo (no de bloques), creado en 1987 por Ronald Rivest (la R de RSA - Secreto Comercial de RSA Data Security). Fue publicado el 13 de Septiembre de 1994 (usando remailers anónimos) en un grupo de news: sci.crypt. Es usado por diversos programas comerciales como Netscape y Lotus Notes.
Funciona a partir de una clave de 1 a 256 bytes (8 a1024 bits), inicializando una tabla de estados. Esta tabla se usa para generar una lista de bytes pseudo-aleatorios, los cuales se combinan mediante la función XOR con el texto en claro; el resultado es el texto cifrado.

Red Inalámbrica (Wireless Network)
También conocida como WLAN o red wireless, permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

Roaming - (Itinerancia)
En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad.

RSA
Es un cifrador simétrico definido en la patente numero 4,405,829 de los Estados Unidos en 1977.
La patente expiró el 20 de Septiembre del 2000.

RSN – Red con seguridad robusta (Robust Security Network)
Protoclo de seguridad del estándard 802.11i.

RSNA
Robust Security Network Association, asociación de seguridad usada en una RSN.

RSN IE
Robust Security Network Information Element, campos que contienen información RSN incluida en Probe Response y Association Request.

**S**

SNIFFER
Proviene de la palabra en inglés “sniff” cuyo significado es olfatear, husmear, escudriñar.

Programa informático cuya finalidad es la de escuchar y escudriñar las transmisiones realizadas en una red, revelando todo lo que pasa en el medio de transmisión. Para hacerlo se escuchan todos los paquetes que viajan en la red, poniendo a la NIC en un modo de escucha denominado “modo promiscuo”. Se pueden capturar datos como nombres de usuarios, contraseñas, nombres de equipos, hacer un mapa completo de la red, estadísticas de uso, tipo de sistema operativo de cada estación, en fin se revela la red en todos sus aspectos.

Los sniffers pueden emplearse tanto con funciones legítimas de monitoreo y administración de red como para el robo de información. Los sniffers no autorizados pueden ser extremadamente peligrosos para la seguridad de una red ya que virtualmente es casi imposible detectarlos y pueden ser emplazados en cualquier lugar, convirtiéndolos en un arma indispensable de muchos piratas informáticos. Algunas herramientas sniffers conocidas son: WepCrack, Airsnort o NetStumbler, entre otras...

Spoof - Engañar ó timar.

Spoofing – Acto en el que un hacker observa y modifica cualquier paquete de datos.

SSID - Identificador de red inalámbrica, similar al nombre de la red pero a nivel WI-FI.

SSL – Capa de Conexión Segura (Secure Sockets Layer)
Aprobado como estándar por el the Internet Engineering Task Force (IETF), es un protocolo desarrollado por Netscape para la transmisión privada de documentos vía Internet cliente/servidor.

Trabaja empleando una llave privada de encriptación de datos que es transferida a través de la conexión SSL. Los navegadores Netscape y Explorer soportan SSL, y muchas páginas web emplean el protocolo para obtener información confidencial del usuario, como números de tarjeta de crédito, etc.... Por convención, las URLs que precisen una conexión SSL comienzan con https, en lugar de http.

**T**

Tarjeta de Red Inalámbrica
Tarjeta típica de red (con conectividad para LAN) pero diseñada y optimizada para entornos inalámbricos. Dependiendo de a quien vaya destinada existen diversos modelos: CompactFlash, PCI, PCMCIA, USB

TMK – Llave temporal MIC (Temporary MIC Key)
Clave para la integridad de datos en tráfico unicast (usada en TKIP).

TK – Llave Temporal (Temporary Key)
Clave para la encriptación de datos en tráfico unicast (usada también para la comprobación de la integridad de datos en CCMP).

TKIP - Protocolo de Integridad de Clave Temporal (Temporal Key Integrity Protocol)
Cifra las llaves utilizando un algoritmo hash y, mediante una herramienta de chequeo de integridad, asegura que las llaves no han sido manipuladas.

TLS - Transport Layer Security
Protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía Internet. Trabaja en dos niveles: El protocolo de registro TLS - situado en el nivel superior de un protocolo de transporte seguro como TCP asegura que la conexión es privada empleado encriptación simétrica de datos y asegura que la conexión es fiable. También se utiliza para la encapsulación de protocolos de nivel superior, tales como el TLS handshake Protocol. Y, el protocolo de handshake TLS - permite la autenticación entre el servidor y el cliente y la negociación de un algoritmo de encriptación y claves criptográficas antes de que el protocolo de la aplicación transmita o reciba cualquier dato. TLS es un protocolo independiente que permite que protocolos de niveles superiores se sitúen por encima de él de manera transparente. Basado en SSL de Netscape 3.0, TLS supercede y es una extensión de SSL, si bien no son interoperables.

TSC – (TKIP Sequence Counter)
Contador de repetición usado en TKIP (al igual que Extended IV).

TSN - Red de Seguridad de Transición (Transitional Security Network)
Sistemas de seguridad pre-802.11i (WEP etc.).

**W**

Warchalking
Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico. Tiene sus antecedentes durante la Gran Depresión del 30 en los Estados Unidos, los desocupados dibujaban símbolos en los edificios para marcar los lugares donde podían conseguir comida.

Wardriving
Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos wireless. Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, patines, etc.

WEP – Privacidad equivalente al cableado (Wired Equivalent Privacy)
Protocolo de encriptación por defecto para redes 802.11.

WPA - Acceso Wi-Fi Protegido (Wi-Fi Protected Access)
Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

WPA2 - Segunda versión de WPA
Protocolo de seguridad para redes Wi-Fi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Puntos de Acceso de última generación.

Warspamming
Acceso no autorizado a una red inalámbrica y uso ilegítimo de la misma para enviar correo masivo (spam) o realizar otro tipo de acciones que comprometan el correcto uso de un sistema.

WEP
Siglas del protocolo "Wired Equivalent Privacy", proporciona transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, ya que hay software dedicado a violar este cifrado, aunque requiere tiempo.

WEP2
Es una modificación del protocolo WEP realizada el año 2001, como consecuencia de una serie de vulnerabilidades que se descubrieron. No obstante, todavía hoy no existe ninguna implementación completa de WEP2.

Wi-Fi Alliance
"The Wi-Fi Alliance" se formó en 1999. Certifica la interoperabilidad de productos WLAN basados en la especificación 802.11.

WIMAX
Siglas de "Worldwide Interoperability for Microwave Access" (http://www.wimaxforum.org), grupo no lucrativo formado en abril de 2003 iniciativa de Intel/Nokia/Fujitsu/entre otras que certifica la interoperabilidad de los productos con tecnología inalámbrica.

WLAN
Siglas de "Wireless Local Area Network" (Ver Red Inalámbrica).

WPA - Acceso Wi-Fi Protegido (Wi-Fi Protected Access)
Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP y la autenticación de usuarios se realiza mediante el protocolo EAP.

WRAP - Protocolo para autenticación robusta inalámbrica (Wireless Robust Authenticated Protocol)
Antiguo protocolo de encriptación usado en WPA2.

WWWD
Siglas de "The WorldWide Wardrive", evento internacional que durante una semana reúne a expertos de todo el mundo que buscan y catalogan nodos inalámbricos en sus ámbitos geográficos (http://www.worldwidewardrive.org/).