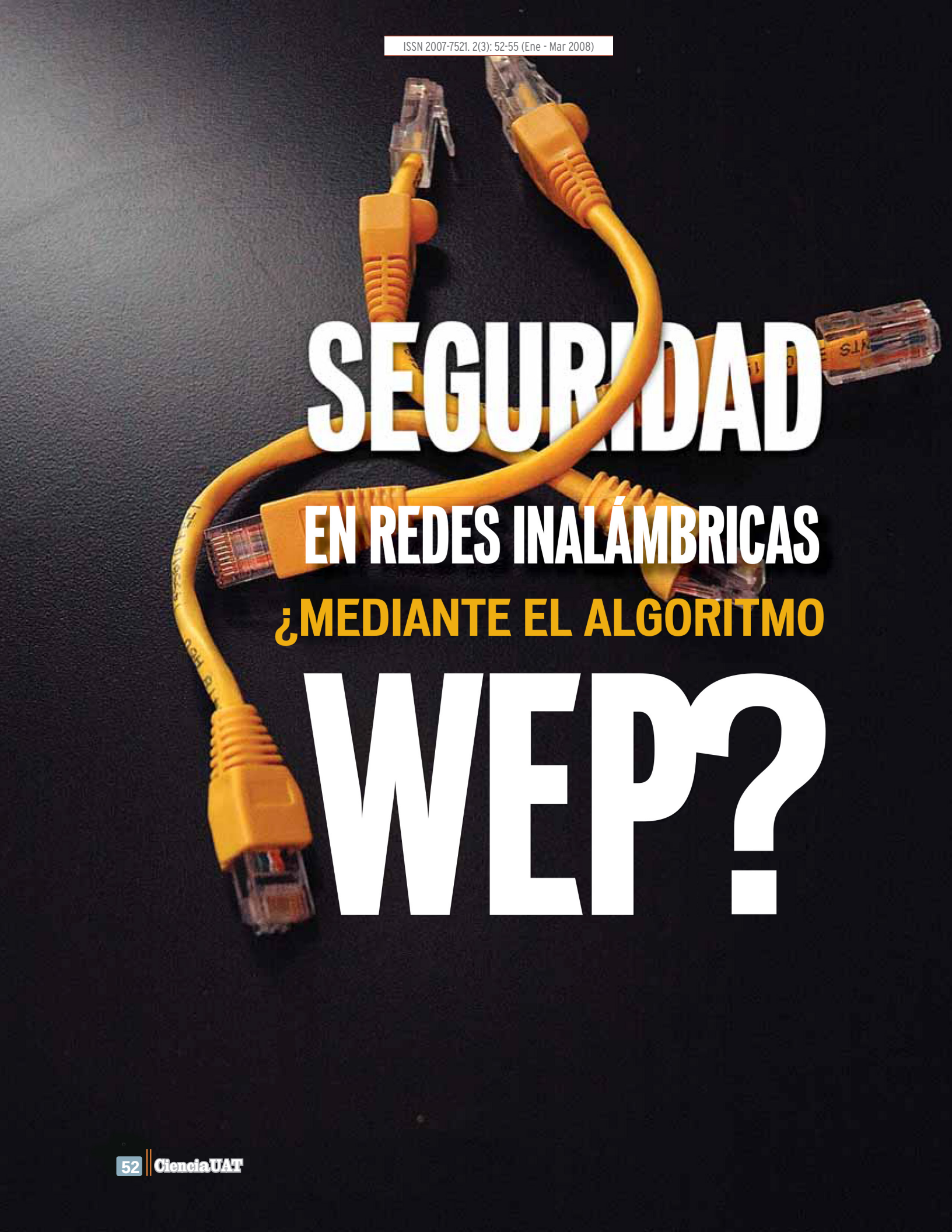
ISSN 2007-7521. 2(3): 52-55 (Ene - Mar 2008)



SEGURIDAD EN REDES INALÁMBRICAS ¿MEDIANTE EL ALGORITMO WEP?

Por Isaac Mata Villalpando Becerra
Alumno de octavo semestre de la Carrera de Ingeniería en Telemática, Unidad Académica Multidisciplinaria Agronomía y Ciencias, Centro Universitario Victoria, UAT

Las redes inalámbricas potenciaron el uso de las computadoras facilitando conectividad, información y datos para el desarrollo

RESUMEN

Las redes inalámbricas al utilizar el aire como medio de transmisión son más vulnerables debido a su facilidad de acceso. Desde que se estableció el estándar IEEE 802.11 en su versión original contempló mecanismos de seguridad, entre ellos el algoritmo opcional WEP, ya que utiliza el RC4 que requiere una secuencia de caracteres (seed) formada por una clave secreta (llave) y un vector de inicialización (IV). Dicho mecanismo de seguridad en la actualidad es el más popular aunque por su estructura no proporciona una adecuada protección, haciendo necesaria la utilización de otros mecanismos más modernos y eficientes.

INTRODUCCIÓN

Las redes de computadoras son una necesidad en nuestra vida diaria, son utilizadas en la industria, los negocios, la salud, la educación y hasta en el hogar. En los 90´s fue el auge de las redes inalámbricas que proporcionan además movilidad y eliminan la necesidad del tendido de cableado.

Al utilizar el aire como medio de comunicación, y que la señal esté disponible en todas direcciones y para todos los usuarios conlleva riesgos que deben ser reducidos. De la necesidad de uniformidad de este tipo de redes para asegurar su interoperabilidad surgió el estándar IEEE 802.11 que las regula, en el que ya se incluían mecanismos para proveer seguridad, este es el algoritmo WEP que en la actualidad es el más popular, aunque presenta graves vulnerabilidades.

DESARROLLO

No cabe la menor duda que el surgimiento de las redes de computadoras ha sido un gran avance del desarrollo humano y su utilidad es indiscutible para el progreso de todas las actividades. Las redes inalámbricas han potenciado un gran dinamismo de actividades hoy en día.[1]

Estas redes son utilizadas con regularidad en nuestra vida diaria porque requerimos de conectividad, información y datos de proceso para el desarrollo óptimo de nuestras labores.[2] Por esta necesidad de utilizar los recursos independientemente de nuestra ubicación geográfica en un momento dado es que surgieron este tipo de redes; en sus inicios enfrentaron graves problemas de compatibilidad, pues los diversos fabricantes expusieron sus soluciones por separado, por ello, hubo la necesidad de estandarizarlas surgiendo así en 1997 el estándar IEEE 802.11.[1]

Fotografías: Demian Ayala

El uso de redes inalámbricas es utilizado cotidianamente, por lo que debe ser un medio seguro de conectividad.

Una red inalámbrica de área local mejor conocida como WLAN está compuesta básicamente de un punto de acceso o AP (Access Point) y de varias terminales móviles con su apropiada interfaz, la tarjeta de red.[3]

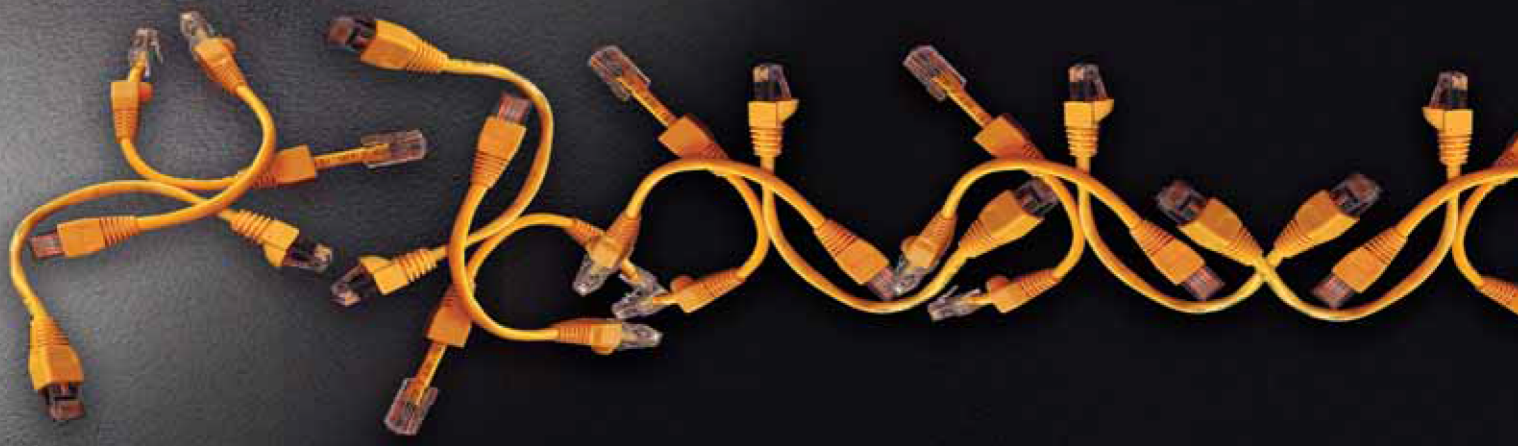
Al poseer estas facilidades y comodidades y que su medio de transmisión sea precisamente al aire trae consigo inevitablemente aspectos importantes de seguridad que deben ser tomados muy encuenta, especialmente si la información transmitida es relevante o si la disponibilidad de nuestra red es primordial.

Estos aspectos de riesgo pueden ser ataques pasivos o activos. Los ataques pasivos son las escuchas indeseadas de lo que está siendo trasmitido; mientras que al hablar de ataques activos nos referimos a aquellos que tienen una incidencia directa sobre el sistema de comunicación, como por ejemplo la utilización de la infraestructura por usuarios no deseados, hasta atentar contra su rendimiento o utilidad, además del acceso a la red cableada con la que una red inalámbrica se conecta.[4]

En los inicios de ésta tecnología los procedimientos y mecanismos de seguridad eran tan débiles que fácilmente fracasaban en su objetivo.1 Consciente de esa problemática, el comité para la estandarización de las WLAN propuso desde su primera edición mecanismos para tratar de mitigar el riesgo, entre ellos el algoritmo opcional WEP (Wire Equivalent Privacy, Privacidad Equivalente a Cable).[5]

A pesar que existen diferentes mecanismos de seguridad en la actualidad, los cuales proporcionan niveles más aceptables de protección como WPA, TKI, CNAC, OSA, etc., el

CienciaUAT. 2(3): 52-55 (Ene - Mar 2008). ISSN 2007-7521



WEP se ha seguido utilizando por la población en general, probablemente por ser el más popular, porque no se tiene conocimientos sobre la materia o porque no cuenta con los recursos necesarios para hacer otras implementaciones. Los nuevos AP soportan WEP sin costo adicional.

WEP es un algoritmo opcional de seguridad para brindar protección a las redes inalámbricas que se ha mantenido sin cambios aún en las posteriores revisiones del estándar 802.11. Fue diseñado para intentar equivaler la privacidad de una red cableada, y no para ser la medida de seguridad, o sea para hacer del medio tan seguro como un cable. La confidencialidad de la información depende del manejo externo de la llave (clave secreta). [6, 7]

CONFIGURACIÓN PARA UTILIZAR EL WEP

Las interfaces gráficas de casi la totalidad de los puntos de acceso disponibles en el mercado nos permiten fácilmente configurar el WEP. La disposición de los controles de las interfaces varía de modelo a modelo y de marca a marca, aún así las diversas interfaces son semejantes y permiten fácilmente ser configuradas. Basta posicionarnos en el apartado de seguridad y habilitar la utilización del WEP y asignarle la llave o "key" y al finalizar guardar los cambios.

En los dispositivos móviles será suficiente encender la antena y buscar la red inalámbrica. Al ser detectada, se deberá intentar acceder. El sistema le pedirá ingresar la llave, la cual es configurada en el punto de acceso respectivo.

CARACTERÍSTICAS Y FUNCIONAMIENTO

El algoritmo WEP utiliza una clave estática (llave) en los dispositivos móviles y el punto de acceso, y en el estándar no se contempla ningún mecanismo para la distribución o generación automática de la llave, lo que obliga a escribirla manualmente en todos los elementos de la red,8 generando así varios inconvenientes pues al estar almacenada en todos los elementos de la red aumenta la posibilidad de ser obtenida, y entre más grande sea la red se necesitará más administración, lo que generalmente provoca que la llave sea poco cambiada o nunca cambie.

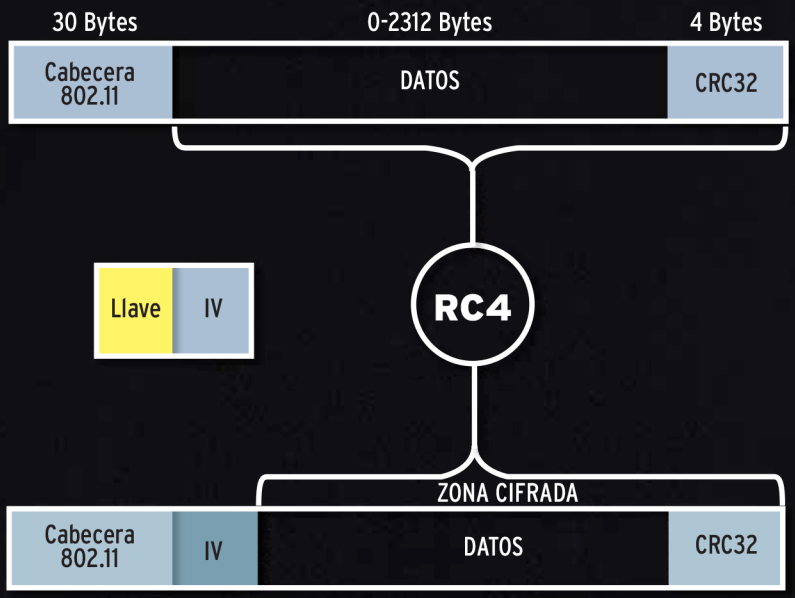


Diagrama del algoritmo WEP

WEP utiliza el algoritmo de encriptación RC4 creado en 1987 por Ronald Rivest de RSA Data Security Inc., utilizando claves "seed" de 64 bits según el estándar, de los cuales 40 bits son la llave manualmente configurada y los 24 restantes el vector de inicialización (IV), el cual es generado dinámicamente y debe ser diferente para cada trama, generado en un extremo y enviado al otro elemento en la misma trama. [5, 7, 8, 9]

El algoritmo de encriptación WEP funciona de la siguiente manera:

1.- Se calcula un CRC de 32 bits de los datos a enviar (método para garantizar la integridad de estos).
2.- Se concatena la llave y el IV para formar una secuencia de caracteres "seed".
3.- El PRNG (pseudo-random number generator) de RC4 genera una secuencia de caracteres (keystream) a partir del seed y del CRC-32 del punto 1.
4.- Se calcula una XOR de los caracteres del punto 1 con los del punto 3, obteniendo así el mensaje cifrado.
5.- En el campo de datos de la trama 802.11 se envían el IV (sin cifrar) y el mensaje cifrado.

DEBILIDADES Y FALLAS DE SEGURIDAD

Que el algoritmo WEP implemente IV acarrea varios problemas de seguridad. Recordemos que el IV es la parte variable del seed cuya finalidad es evitar que un atacante recopile información suficiente para descifrar la llave y que, además viaja sin cifrar en todas las tramas.

Dada su longitud de 24 bits solamente existen 16 millones 777 mil 216 valores posibles para el IV, por lo que sus valores terminan repitiéndose en cuestión de minutos y entre más tráfico exista en la red el tiempo tiende a ser menor.

Un atacante aplicando el algoritmo WEP de manera inversa puede llegar a descifrar la llave que le fue asignada a la red y así tener acceso total como cualquier usuario legítimo. El estándar 802.11 no especifica cómo manejar el IV, sólo indica que se debería de cambiar para cada trama pero no obliga a ello, dejando en manos de los fabricantes la variación del mismo. A consecuencia de ésto generalmente se optó por una solución sencilla: cada vez que una tarjeta de red es iniciada se asigna el valor de 0 al IV y se incrementa en 1 para cada trama. [7]

Todo lo anteriormente dicho nos lleva a afirmar que el algoritmo WEP es una solución de seguridad bastante insegura e inconveniente a las necesidades prácticas, pues evidentemente resulta fácil llegar descifrar la llave y tener así acceso a la red inalámbrica.

RECOMENDACIONES

Cuando no se esté utilizando o durante los períodos en que no deba ser utilizada apaga tus puntos de acceso.

Modificar todas las configuraciones por defecto de los puntos de acceso como el SSID (identificador de servicio), la contraseña del administrador y el canal de transmisión, pues son bastante conocidos e incluso pueden formar parte de una herramienta para realizar ataques.

Se recomienda cambiar configuraciones y contraseña de acceso, así como mantener actualizado el software para soporte de nuevas tecnologías.

Si se cuenta con la infraestructura necesaria es ampliamente recomendable conectar todos los puntos de acceso a una subred o VLAN (Virtual Local Area Network) diferente y utilizar un Firewall entre la red cableada y la inalámbrica.

Es una buena opción mantener actualizado el software del hardware para así tener soporte a nuevas tecnologías que brinden un mayor grado de seguridad y utilizar estas nuevas tecnologías para tal efecto. [9]

Complementarse con otros mecanismos de seguridad de más alto nivel como VPN (Virtual Private Network).

CONCLUSIONES

En la actualidad la utilización de redes son menesteres en nuestras actividades diarias y las redes inalámbricas las potencian pero su utilización implica riesgos que deben ser mitigados.

El algoritmo opcional WEP estipulado en el estándar original 802.11 que en posteriores revisiones no ha sufrido modificaciones, lo que lo vuelve obsoleto, intenta brindar características semejantes de seguridad a una red cableada, sin embargo aunque su concepción fue buena, en la actualidad no es recomendable su uso como medida de seguridad pues dada su estructura presenta graves vulnerabilidades. A pesar de esto, es en la actualidad el más utilizado por la población en general, pero es recomendable tomar las precauciones debidas e implementar otros mecanismos más recientes a fin de proteger mejor nuestra información e infraestructura.

BIBLIOGRAFÍA

1 CUELLAR RUIZ Jaime (2004) "Redes Inalámbricas. Estándares y Mecanismos de Seguridad" Disponible en http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm

2 BARAJAS Saulo (2004) "Protocolos de Seguridad en Redes Inalámbricas" Disponible en http://www.saulo.net/pub/inv/SegWiFi-art.htm

3 Universidad INCCA de Colombia "Redes Locales Inalámbricas" Disponible en http://www.unincca.edu.co/boletin/indice.htm

4 BORISOV Nikita, GOLDBERG Ian y WAGNER David "Security of the WEP Algorithm" Disponible en http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

5 LAN MAN Standards Committee of the IEEE Computer Society (2003) "ANSI/IEEE Std. 802.11, 1999ed (r2003) Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications."

6 DEL RAZO Minerva (2004) "Redes Inalámbricas" Disponible en: http://www.tress.com.mx/boletin/junio2004/redes.htm

7 TANENBAUM, Andrew S. Redes de computadoras. 4° ed. México: Pearson, 2003.

8 GARCÍA TOMÁS Jesús, RAYA CABRERA José Luis, RODRIGO RAYA Víctor. Alta velocidad y calidad de servicio en redes IP. México: Alfaomega, 2002.

9 CISCO SYSTEMS, INC. Academia de networking de Cisco Systems Guía del primer año CCNA 1 y 2. 3°ed. España: Pearson, 2004.

AGRADECIMIENTOS

Al Creador por concederme cada día lleno de optimismo y renovada energía. A MC. Mariby Lucio Castillo por incitarme a realizar investigación, al Dr. Manuel Aguirre Bortoni por apoyarme en la edición y a M.A. Lucía Calderón Santos por las facilidades otorgadas.

Contacto:
Cel: 834 102 5411
Email: it.isaac@hotmail.com
Dirección de informática
Edificio Centro de Excelencia, 2do. piso
ext. 2824
Email: imata@uat.edu.mx