MECANISMOS DE SEGURIDAD EN REDES INALÁMBRICAS

Manuel Suárez Gutiérrez

RESUMEN

La popularización en el uso de redes inalámbricas (WLAN), se debe principalmente, a que en ocasiones, resulta ser más económica y fácil de instalar que las redes cableadas.

Esto, ha originado que los usuarios de las mismas exijan mayor seguridad tanto en la integridad de la información, como en la autentificación de nodos o usuarios de la red, por lo que este documento pretende abarcar diferentes mecanismos de seguridad utilizados actualmente en la comunicación de WLAN's.

ABSTRACT

The popularity in the use of wireless networks (WLAN), must principally, to that in occasions, it turns out to be economic and easy to install than wired networks.

This has originated that the users of the same ones demand greater security in the integrity of the information, and authentication of nodes or users of the network, reason why this document tried to incorporate the different mechanisms from security used in these days in the communication of WLAN's.

Introducción

La tecnología esta cambiando de forma acelerada, haciendo que en algunos casos, las redes sean la herramienta primordial para comunicarnos. Es por ello que la propia movilidad que tenemos, ha hecho necesario la evolución de las redes cableadas a inalámbricas.

Los sistemas de redes y Telecomunicaciones actualmente están sujetos a una innovación tecnológica altamente cambiante, trayendo consigo, que los sistemas basados en la comunicación inalámbrica no sean la excepción, por lo que evolucionan rápidamente.

Las redes inalámbricas fueron creadas por la necesidad de proveer acceso a las redes por medio de dispositivos de computo portátiles, lo cual evidentemente atrajo problemas hacia el medio de transmisión, debido a los intrusos que pueden entrar en la red libremente dando una posibilidad virtual de no ser detectados. Es por ello, la importancia de tener comunicaciones seguras en redes inalámbricas para establecer enlaces de intercambio de información confidencial. [2]

Las redes inalámbricas en los últimos años, han tenido un auge muy importante por lo que los mecanismos de seguridad que se desarrollaron en un inicio, rápidamente pasaron a ser superados por aquellos usuarios mal intencionados, los cuales buscan por donde penetrar a los sistemas en las vulnerabilidades de seguridad que estos presentan.

Esto originó, que los fabricantes de dispositivos inalámbricos y a organizaciones como la IEEE (Institute of Electrical and Electronics Engineers) a buscar las alternativas de solución a estos problemas.

Desde que se comenzó a investigar en está área, se han encontrado varias soluciones las cuales, se han ido implantando, tal como es el caso del

mejoramiento de la encriptación WEP (Wired Equivalent Piracy) la cual, en su forma mas básica de codificación es de 40 bits, sin embargo, para lograr una mayor seguridad, se ha extendido hasta los 128 bits. [3] [2]

¿Qué es una red inalámbrica?

Las comunicaciones entre dispositivos de cómputo han tenido un gran auge [7], haciendo posible que el medio de transmisión utilizado para realizar las conexiones entre cada uno de los diferentes dispositivos de cómputo [6], evolucione rápidamente, teniendo como resultado que en la actualidad las redes inalámbricas se acoplen más al estilo y ritmo de vida de los usuarios.

Dado lo anterior se hace necesario definir el significado de una red inalámbrica, la cual, es aquella que permite a sus usuarios conectarse a una red local o la Internet, sin la necesidad de usar cables, debido a que las transacciones realizadas o paquetes de información, se transmiten mediante ondas electromagnéticas, propagadas utilizando como medio de transmisión el aire. [2]

Esto quiere decir que una red Inalámbrica, es aquella en la cual, voz y datos pueden ser transmitidos de un punto a otro sin la necesidad de utilizar un medio físico, como es el caso del cable de cobre o la fibra óptica, lo cual, la hace muy atractiva para los usuarios finales. [4]

Un equipo es inalámbrico si tiene la capacidad de moverse libremente alrededor de una red de área local (LAN) o amplia (WAN), sin la necesidad de utilizar ningún medio físico para conectarse, lo cual permite a los usuarios acceder electrónicamente en cualquier lugar y momento a la información y servicios provistos en la red. [5]

Las redes inalámbricas están geográficamente divididas en células, donde cada una de ellas contiene un Access Point, los cuales se conectan por cables, ya sean de cobre o ópticos, a la infraestructura de la red. [5]

El diagrama básico de una red inalámbrica de área local (WLAN), se muestra en la Figura 1, consistiendo de un punto central llamado Access Point, el cual transmite información entre diferentes nodos de la WLAN, haciendo posible la comunicación de los nodos hacia otras redes. [6], [7]

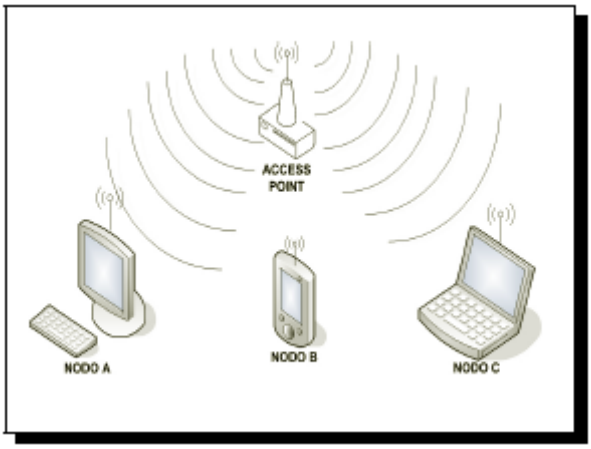

Figura 1: Red Inalámbrica de Área Local (WLAN).

También la Figura 1, muestra algunos de los dispositivos que se utilizan comúnmente como nodos de una WLAN, los cuales pueden ser una computadora de escritorio, una PDA (Personal Digital Assistant), así como una computadora portátil también conocida como Laptop.

Una Computadora de escritorio (PC), es aquel equipo de cómputo que por sus características físicas, no posee la capacidad de moverse entre células inalámbricas, por lo que es más factible que funcione por medio de una red cableada. Sin embargo puede trabajar con una WLAN si esta posee una tarjeta de red inalámbrica, en la Figura 2 se muestra un ejemplo de este adaptador de red.

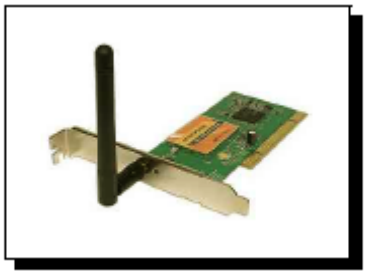

Figura 2: Tarjeta de Red Inalámbrica para PC.

Una PDA, la cual se muestra en la Figura 3, realiza funciones básicas de cómputo, aunque en sus inicios era utilizada específicamente como agenda electrónica. Actualmente presentan características como la de tener acceso a Internet y conexiones de red, lo cual permite que este dispositivo a pesar de tener ciertas limitantes por su capacidad de procesamiento satisfaga las necesidades básicas de los usuarios.

Figura 3: PDA

Una Computadora portátil, es aquel equipo de cómputo que tiene la capacidad de viajar entre las células inalámbricas, donde la tarea de reenviar la información entre una red cableada y una computadora portátil debe transferirse a una nueva célula de un Access Point, en la Figura 4, se muestra un Access Point para uso domestico, y un Access Point utilizado a nivel empresarial. [5]

(a) Modelo WRT300N Wireless-N Broadband Router de la Marca LINKSYS.

b) Modelo Cisco Aironet 1240AG.

Figura 4: Access Points utilizados a nivel residencial y empresarial.

Las redes inalámbricas, no fueron diseñadas con el propósito de proporcionar una seguridad robusta para realizar los intercambios de información entre los nodos y el Access Point. Esto se ve reflejado en las limitaciones de seguridad dadas en el diseño del protocolo, las cuales, han sido explotadas por individuos mal intencionados, dando como resultado que las WLAN no sean confiables, lo cual a hecho que se realicen esfuerzos sustanciales para asegurar el acceso a las WLAN así como también el paso a través de ella, mediante la denegación del acceso a dichos usuarios. [4]

Dentro de las WLAN existen varios mecanismos de seguridad de los cuales los más utilizados son:

- SSID (Service Set Identifier): Consiste en que el cliente debe de tener configurado el mismo SSID que el Access Point.
- WEP (Wired Equivalet Piracy): Su objetivo principal consiste en proveer la confidencialidad de la transmisión de la información, tal como se ofrece en las LAN.

- Filtrado por dirección MAC: El Access Point esta configurado para aceptar solo las peticiones de ciertos nodos de la red.
- WPA (Wi-Fi Protected Access): Distribuye claves diferentes a cada usuario, mejora la integridad de la información, al igual que WEP, los usuarios mal-intencionados pueden obtener su clave, otra de sus desventajas es que al tener una contraseña de al menos veinte caracteres, la cual es difícil que los usuarios la recuerden. [8]

Categorías de las Redes Inalámbricas

Las redes inalámbricas se catalogan de acuerdo a 3 categorías, las PAN (Redes de Área Personal), LAN (Redes de Área Local), WAN (Redes de Área Amplia).

PAN: Dentro de las PAN, se encuentran las redes inalámbricas que utilizan la tecnología Bluetooth, la cual posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia a 2.4 GHz en la banda ISM, ofreciendo la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales. Así mismo, estas redes utilizan el estándar de la IEEE 802.15.1 aprobado en el año 2002. [11]

Algunos de los dispositivos que utilizan esta tecnología para crear una PAN son las Agendas Electrónicas Personales (PDA), Teléfonos Celulares, Impresoras, Mouse, Teclado, Cámaras Fotográficas Digitales, GPS, entre otros. Los cuales se muestran en la Figura 5.

(a) Palm Tungsten.

(b) Teléfono Celular Motorota V3.

(c) Mouse marca Targus.

(d) Impresora Marca Hp.

Figura 5: Dispositivos que utilizan la tecnología Bluetooth.

WLAN: Las LAN inalámbricas son conocidas por el nombre de WLAN, las cuales permiten una gran flexibilidad y portabilidad cosa que las redes de área local (LAN) cableadas tradicionales no permiten. [1]

La principal diferencia entre LAN tradicionales y una WLAN es que las LAN requieren conectar a los usuarios de cómputo a una red mediante cableado a un Switch, mientras que una WLAN, no solo conecta equipo de cómputo sino que también admite otros componentes a la red mediante el uso del Access Point. [1]

Las WLAN se pueden configurar de dos modos:

- Ad-Hoc: esta configuración soporta una organización propia en infraestructuras de redes inalámbricas. Así mismo, el organismo encargado de ver todo lo relacionado con este tipo de red inalámbrica es el grupo de trabajo de la IETF's llamado Mobile Ad Hoc Networks (manet). [12]

  Una red Ad-Hoc, consiste de plataformas inalámbricas, las cuales son libres de movimiento arbitrariamente. A cada una de estas plataformas se le denomina como "nodos", el cual consiste en dispositivos de red separados físicamente o que puede estar integrado en un dispositivo como es una computadora portátil o una PDA. Los nodos están equipados con un transmisor y receptor inalámbrico los cuales pueden ser omni-direccionales, altamente direccionales, orientables o una combinación de ellos. [12]

  En resumen, este tipo de redes inalámbricas consisten en que nodos inalámbricos, los cuales se comunican directamente mediante su tarjeta de red inalámbrica, teniendo como limitante la distancia de cobertura entre los dispositivos en la red. La Figura 6 ilustra el esquema de la topología ad-hoc. [12]

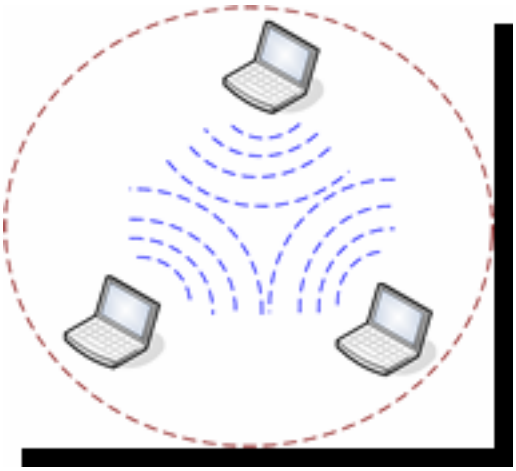

Figura 6: WLAN con topología Ad-Hoc.

- Punto de Acceso o Access Point: Un Access Point se comunica con dispositivos equipados con un adaptador de red inalámbrica, logrando conectar estos dispositivos con la red cableada.

  Un Access Point, hace las veces de repetidor inalámbrico. En este tipo de redes, se requiere de una planificación muy cuidadosa y compleja, ya que los puntos de acceso deben distribuirse estratégicamente para evitar que algunas zonas se queden sin cobertura, evitar obstáculos, asegurar un ancho de banda mínimo para cada usuario, etc. [1]

  Sin embargo, a pesar de ser complejas, ofrecen muchas ventajas. Una de las más importantes es la libertad de movimiento, donde un usuario conectado a un Access Point puede desplazarse libremente por la zona de cobertura de la red, la cual es aproximadamente 100 metros (arriba de 300 pies), de modo que sí en algún momento, abandona dicho Access Point y pasara al área de cobertura de otro, las conexiones se mantendrían (roaming). [1]

En la Cuadro 1, se muestran las características principales de las WLAN.

Característica	**Descripción**
Capa Física	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), Infrarojos (IR).
Banda de Frecuencia	2.4 GHz y 5GHz
Tasa de Transferencia	1 Mbps, 2Mbps, 5.5 Mbps, 11 Mbps, 54 Mbps
Seguridad de Datos y Red	Se basa en el algoritmo de cifrado RC4 para confidencialidad, autenticación e integridad. Se limita por la administración de claves.
Rango de Operación	100 metros
Aspectos Positivos	Se obtiene una velocidad de Ethernet sin usar cables,

	una variedad de productos y compañías, los costos están disminuyendo.
Aspectos Negativos	Poca seguridad, la tasa de transferencia disminuye con la distancia y carga.

Cuadro 1: Características Principales de las WLAN. [1]

WAN: En las WAN inalámbricas, se utiliza WiMAX, la cual propone mayores anchos de banda en dispositivos portátiles y puntos de acceso inalámbricos basados en IP en la comunicación de redes remotas [13], así mismo, WiMAX, esta regido por el estándar IEEE 802.16 el cual utiliza las bandas de frecuencia entre los 2 y 11 GHz obteniendo una cobertura de hasta 70 Km [14].

En la primera versión publicada por la IEEE en el estándar 802.16a, se menciona que WiMAX está diseñada para funcionar por debajo de los 11 GHz y no es necesario que disponga de visión directa entre las antenas. Puede dar un ancho de banda de 75Mbps y aunque su radio de cobertura puede llegar hasta los 50 km los valores medios están pensados entre los 7 km y los 11 km.

El grupo encargado de realzar las investigaciones, certificaciones, foros, cursos, congresos, así como publicar todas las noticias concernientes a esta tecnología es ”IEEE and WiMax Forum”. [20]

Rango de Cobertura de las WLAN’s

La cobertura confiable para el estándar 802.11 de las WLAN’s depende de varios factores, incluyendo la tasa de transferencia requerida y capacidad, fuentes de interferencia de radio frecuencias, área y características físicas, potencia, conectividad y por ultimo el uso de la antena. Teóricamente los rangos son desde 29 metros a una velocidad de 11 Mbps en un área cerrada hasta 485 metros a una velocidad de 1 Mbps en un área abierta. Mientras que en un análisis empírico, los rangos varían desde 50 metros en interiores a 400 metros en exteriores, por lo que

hace que las WLAN's sean ideales para diversas aplicaciones. Es importante reconocer que si se añaden antenas especiales con alta ganancia, se puede incrementar el rango de cobertura a varios kilómetros. La Figura 7, muestra los rangos de cobertura dependiendo de la ubicación del Access Point. [1]

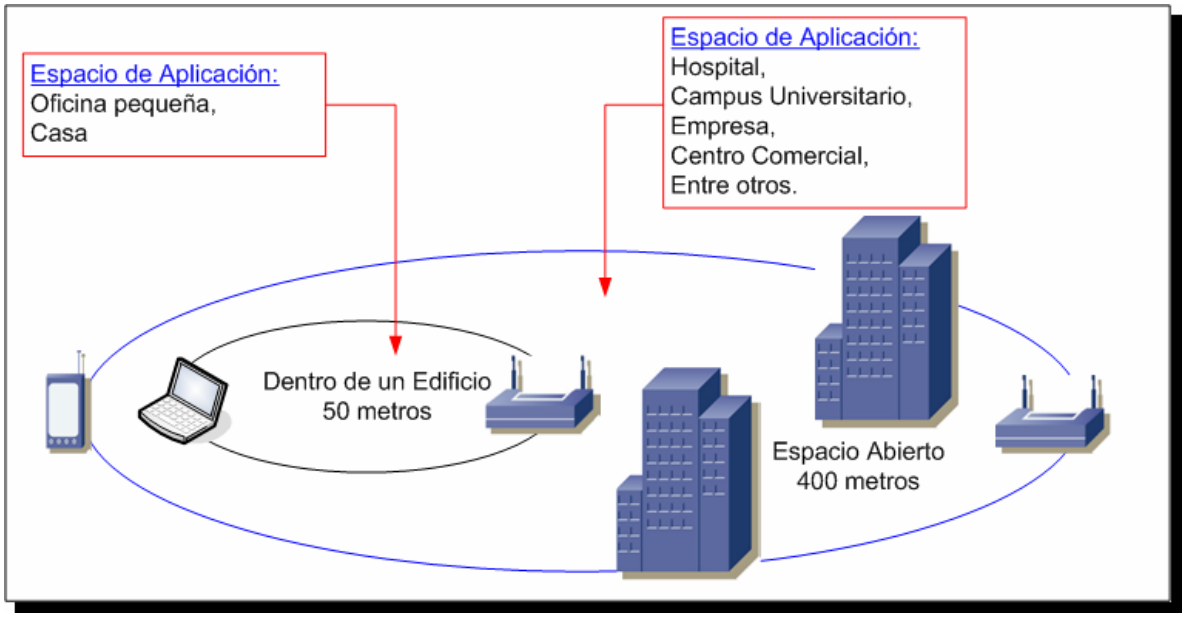

Figura 7: Rango Típico de Cobertura de una WLAN.

Beneficios de las WLAN's

Las WLAN's se caracterizan por tener los siguientes beneficios:

- **Movilidad del usuario**: Los usuarios pueden acceder a archivos, recursos de la red, y a Internet sin la necesidad de tener ninguna conexión física a la red, por lo que los usuarios se pueden desplazar dentro del área de cobertura teniendo una alta velocidad de transferencia de datos.
- **Instalación Rápida**: El tiempo requerido para instalar las WLAN's es relativamente corto dado que el numero de conexiones son hechas sin tener que mover o añadir cableado, tal como sería modificar la infraestructura física de donde se requiera instalar la red.
- **Flexibilidad**: Este beneficio lo notan las empresas que requieren de alto movimiento de usuarios ya que con mover la posición del Access Point

cubren la zona en la que se mueven los usuarios, un ejemplo seria en las conferencias, salas de juntas, etc.

- **Escalabilidad**: Las topologías de red de la WLAN pueden ser fácilmente configuradas para una aplicación en específica de acuerdo a las necesidades de la instalación, para escalar de una red pequeña de punto a punto a una red empresarial que permita roaming sobre un área de cobertura.

Seguridad en las WLAN's

La seguridad en las WLAN se rige por el estándar IEEE 802.11 identifica varios servicios para proveer un ambiente seguro de operación, dentro de los cuales el más difundido es el protocolo WEP (Wired Equivalent Privacy), el cual es usado para proteger el nivel de enlace de datos durante una transmisión inalámbrica entre los clientes y el Access Point. WEP no provee seguridad de punto a punto, solo la provee en la porción del enlace inalámbrico, tal como lo muestra la Figura 8. [1]

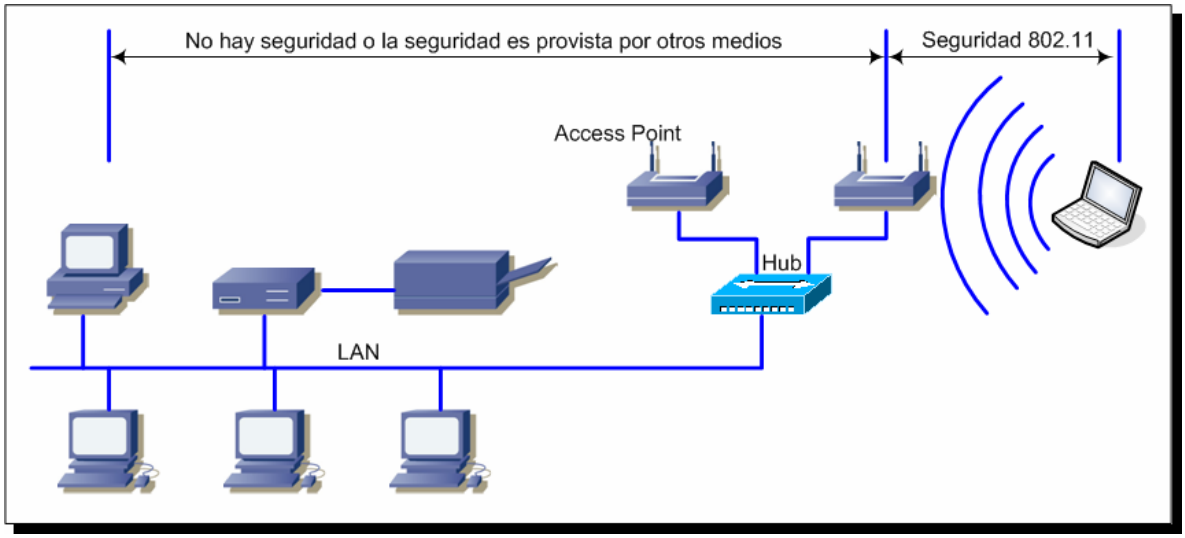

Figura 8: Seguridad Inalámbrica del 802.11 en una Red Típica. [1]

Protocolos usados en la seguridad de WLAN

IEEE 802.11: Es el estándar de la IEEE 802.11 propone tres servicios básicos de seguridad para el entorno de las WLAN los cuales son descritos en la Cuadro 2.

RC4: Es el sistema de cifrado de flujo en aplicaciones de software utilizado más ampliamente. Entre numerosas aplicaciones este codificador es usado para proteger el tráfico de Internet como parte del SSL y esta integrado dentro de Microsoft Windows, así mismo, es parte de los protocolos de cifrado más comunes como WEP, WPA para tarjetas inalámbricas. [15]

RC4 fue diseñado por Ron Rivest en 1987. RC4 tiene un estado interno secreto, el cual funciona como una permutación de todas las N = 2n donde n son los bits de las palabras asociadas con dos índices. [15]

Servicios Básicos de Seguridad	Descripción
Autenticación	Provee servicios de seguridad para verificar la identidad entre las estaciones clientes que se comunican. Esto provee control de acceso a la red denegando acceso a las estaciones clientes que no pueden ser autentificadas propiamente.
Confidencialidad	Provee privacidad lograda por una red cableada. Lo que pretende es prevenir el compromiso de la información de un ataque pasivo.
Integridad	Este servicio asegura que los mensajes no son modificados en el transito entre los clientes Inalámbricos y el Access Point en un ataque activo.

Cuadro 2: Servicios básicos de seguridad para el entorno de las WLAN. [1]

RC4 genera un flujo pseudoaleatorio de bits (un keystream), el cual para cifrar un texto se combina con él usando la función XOR. [15]

Para generar el keystream, el algoritmo de cifrado tiene un estado interno secreto que consiste en una permutación de todos los 256 posibles símbolos de un byte de longitud (llamado ”S”) y de dos índices-apuntadores de 8 bits (llamados ”i” y ”j”). [15]

Para iniciar la permutación se utiliza una clave de longitud variable entre los 40 y 256 bits, el cual lo obtiene mediante un KSA (Key scheduling algorithm), posteriormente se genera el flujo de bits cifrados mediante un algoritmo PRGA (pseudo-random generation algorithm). [15]

Principales mecanismos de seguridad usados en las WLAN

WEP (Wired Equivalent Privacy): Es el algoritmo opcional de seguridad establecido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. [3]

El propósito de la encriptación WEP es incrementar el nivel de seguridad para aquellos dispositivos habilitados con WEP, con la finalidad de obtener el mismo nivel de seguridad que los dispositivos en redes cableadas. Es por ello que la información protegida por WEP, es cifrada con la finalidad de dar confidencialidad y un contador previniendo que los paquetes sean modificados por atacantes activos, así como verificar que solo los usuarios autentificados son los que reciben el servicio de la WLAN. [2]

WEP, fue diseñado con las objetivos de implementarse sobre hardware cuyo costo no fuera elevado, así como también contar con una administración fácil y sencilla, donde cada dispositivo configurado por WEP usaría una Clave, la cual funciona como una contraseña de acceso a la red. Esta Clave es utilizada en todos los dispositivos que están autorizados para comunicarse dentro de la red

administrada por el Access Point, con lo cual se logra que los dispositivos que no cuenten con está Clave no accedan a la WLAN. [2]

La funcionalidad de esta clave en WEP es que se utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca. [3]

Cada nodo en el estándar IEEE 802.11 puede ser configurado con 4 claves simétricas WEP, las cuales son usadas para la encriptación y decriptación de los mensajes WEP. Cada nodo tiene una de estas cuatro claves WEP designadas como “default key”, la cual es usada para cifrar todos los mensajes que van a ser transmitidos por el nodo. Cada mensaje cifrado con WEP tiene 2 bit en el campo del encabezado que contiene el índice de la clave que fue usado para cifrar el mensaje. [3]

El estándar IEEE 802.11 utiliza el protocolo WEP para la confidencialidad de la información. Desafortunadamente, la integridad de la información es vulnerable a los ataques y sus mecanismos de autentificación pueden ser vencidos. Además de que el protocolo de encriptación usado en WEP ha sido comprometido seriamente y los Software de ruptura de Claves WEP son ampliamente difundidos en Internet. [3], [9]

WEP fue diseñado para proveer seguridad utilizando el algoritmo de cifrado RC4 (Rivest Code 4), el cual es un generador aleatorio, también conocido como generador de Claves de Flujo, desarrollado por RSA Laboratories por Ron Rivest

en 1987. Este algoritmo toma una entrada relativamente corta, produciendo como salida una salida más grande llamada Clave Pseudo Aleatoria de Flujo. La Clave RC4 se concatena con el Vector de Inicialización (IV), el cual tiene una longitud de 24 bits y con una de las cuatro claves secretas compartidas por el administrador de la red. [3], [10]

El algoritmo de encriptación RC4 con claves (seed), utiliza según 64 bits, los cuales están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente.

El IV, en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave.

Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante. [3]

El algoritmo de encriptación de WEP es el siguiente:

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, Integrity Check Value).
2. Se concatena la clave secreta a continuación del IV formado el seed.

3. El PRNG (Pseudo-Random Number Generator) de RC4 genera una secuencia de caracteres pseudoaleatorios (keystream), a partir del seed, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (frame body) de la trama IEEE 802.11.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocería el IV y la clave secreta, tendría entonces el seed y con ello podrá generar el keystream. Realizando el XOR entre los datos recibidos y el keystream se obtendrá el mensaje sin cifrar (datos y CRC-32). [3]

Algunas debilidades en RC4 son que el primer byte de la Clave de flujo revela información acerca de la clave secreta, por lo que esto puede ser explotado mediante un ataque planeado, el cual con obtener el suficiente numero de paquetes cifrados buscando mensajes con el mismo IV, con lo que el atacante puede obtener la clave secreta byte por byte. El ataque solo requiere entre 1,000,000 y 5,000,000 paquetes para tener éxito. [3]

WPA (Wi-Fi Protected Access): WPA soluciona gran parte de las debilidades conocidas de WEP y se considera suficientemente seguro.

WPA se distingue por tener una distribución dinámica de claves, utilización más robusta del vector de inicialización y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

- **IEEE 802.1X:** Estándar del IEEE que proporciona control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas

conexiones de un Access Point con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del Access Point. El Access Point mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros). [16], [17]

- **EAP (Extensible Authentication Protocol):** Definido en el RFC 2284 como el protocolo de autentificación extensible, el cual tiene como propósito llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN). [16]

- **TKIP (Temporal Key Integrity Protocol):** Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama. [18]

- **MIC (Message Integrity Code):** Código que verifica la integridad de los datos de las tramas. [18]

WPA2 o IEEE 802.11i: Incluye un algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. El cual, requiriere un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos anteriores a su publicación no poseen las capacidades suficientes de proceso para incorporarlo. [19]

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Counter- Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de los códigos MIC. [19]

Conclusiones

El ser humano por su naturaleza es libre y la necesidad de utilizar cables para poder comunicarse lo limita. Es por ello, que al comercializarse las redes inalámbricas, tuvieron una gran aceptación por parte de los usuarios, dado que esto les permitía moverse y comunicarse libremente en un área en la cual contarán con esté servicio.

A medida que se han empezado a utilizar cada día más estas tecnologías, se hace necesario implementar sistemas y mecanismos mas seguros, los cuales permitirán la autenticación de usuarios así como la confidencialidad e integridad de la información, requeridos para mantener comunicaciones seguras por una red inalámbrica.

Es por ello la importancia de mencionar los mecanismos de seguridad más difundidos en las redes inalámbricas, con la finalidad de que el encargado de administrar la misma, pueda escoger la que más se adecue a las necesidades y requerimientos, que los usuarios soliciten.

Asimismo, es prudente mencionar que aparte de utilizar alguno de los mecanismos de seguridad ya sea WEP, WPA o WPA2, es altamente recomendable, realizar un filtrado de acceso a la red mediante direcciones MAC, las cuales permitirán que solo los equipos registrados en la tabla de acceso puedan ingresar a la red.

Sin embargo, el filtrado por direcciones MAC no es perfecto, dado que existen técnicas como la clonación de direcciones MAC, por lo que está técnica no es 100% segura, haciendo recomendable utilizar alguno de los mecanismos de seguridad mencionados anteriormente, lo cual haría más robusta la seguridad de la red inalámbrica.

Bibliografía

[1] Les Owens Tom Karygiannis. Wireless network security 802.11, Bluetooth and handheld devices. NIST (National Institute of Standards and Technology), pages 1–130, 2002.

[2] Aviel D. Rubin Adam Stubblefield, John Ioannidis. A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). ACM Transactions on Information and System Security (TISSEC), 7:319–332, May 2004.

[3] Avishai Wool. Lightweight key management for IEEE 802.11 Wireless LAN's with key refresh and host revocation. Wireless Networks, 11:677–686, 2005.

[4] Kindervag John. The five myths of wireless security. Information Systems Security, 15:7–16, September 2006.

[5] Hala Elaarag. Improving TCP performance over mobile networks. ACM Computing Surveys, 34:357–374, September 2002.

[6] T. Andrew, Yang Yasir Zahur. Wireless LAN security and laboratory designs. Journal of Computing Sciences in Colleges, 19:44–60, 2004.

[7] Joseph Pasquale Et Al. David Clark. Strategic directions in networks and telecommunications. ACM Computing Surveys, 28:279–290, December 1996.

[8] Mario García, Ross Hytnen. An analysis of wireless security. Journal of Computing Sciences in Colleges, 21:210–216, April 2006.

[9] Yi-wen Liu Jyh-Cheng Chen, Ming-Chia Jiang. Wireless LAN security and IEEE 802.11. Wireless Communications IEEE, 12:27–36, February 2005.

[10] Smyth Elaine Curran Kevin. Demonstrating the wired equivalent privacy (WEP) weaknesses inherent in Wi-Fi networks. Information Systems Security, 15:17–38, September 2006.

[11] Nevo R., Lansford J., Stephens A. Wi-fi (802.11b) and Bluetooth: enabling coexistence. Network, IEEE, 15:20–27, September/October 2001.

[12] G.H. Cirincione M.S. Corson, J.P. Macker. Internet-based mobile ad-hoc networking. IEEE Internet Computing, 3:63–70, 1999.

[13] Teri Robinson. Wimax to the world? netWorker, 9:28–34, 2005.

[14] Michel Barbeau. Wimax/802.16 threat analysis. Proceedings of the 1st ACM international workshop on Quality of service And security in wireless and mobile networks, pages 8–15, 2005.

[15] I. Mantin. A practical attack on the fixed RC4 in the wep mode. Internacional Association for Cryptologic Research, pages 395–411, 2005.

[16] Network Working Group. Rfc 2284 - ppp extensible authentication protocol (eap). http://www.faqs.org/rfcs/rfc2284.html.

[17] Network Working Group. Remote authentication dial in user service (radius). http://www.ietf.org/rfc/rfc2865.txt.

[18] Wireless Fidelity Alliance. http://www.wi-fi.org.

[19] National Institute of Standards Computer Security Resource Center and Technology. http://csrc.nist.gov.

[20] WiMAX Forum. http://www.wimaxforum.org/home/