Universidad Latinoamericana de Ciencia y Tecnología

ULACIT

Licenciatura en Redes y Sistemas Telemáticos

Seminario de Graduación

Articulo Científico

Seguridad Informática: "Una visión general de las aplicaciones y tendencias del mercado para Redes Inalámbricas".

Profesor

Lic. Miguel Pérez

Elaborado por

Duván Castro Jiménez

6 – 277 - 401

01 de Septiembre de 2005

Seguridad Informática: “Una visión general de las aplicaciones y tendencias del mercado para Redes Inalámbricas”.

"A general vision of the applications and tendencies of the market for Wireless Networks."

Duván Castro Jiménez.[1]

[1] Bachiller en Ingeniería Informática. Candidato a Licenciatura en Redes y Sistemas Telemáticos, ULACIT. Correo electrónico: dgcastro@costarricense.cr

Resumen

La problemática que presentan las redes inalámbricas en cuanto a seguridad y confiabilidad es un tema de gran interés para los profesionales y empresas en general, los mismos han de comprender que la seguridad de nuestra red se fundamenta en la correcta evaluación, administración y control de riesgos, en conjunto con el uso de mecanismos de autenticación y encriptación tales como WEP, WAP, VPN, 802.1x, entre otros. Estos nos brindan diferentes niveles de protección y su funcionamiento óptimo depende de la forma en que sean utilizados dentro del sistema estructurado de seguridad.

Palabras claves

Seguridad Informática, Seguridad en redes, Redes Inalámbricas, Mecanismos de Autenticación y Encriptación.

Abstract

The problem that present the wireless networks as for security and confiability is a topic of great interest for the professionals and companies in general, the same ones must understand that the security of our network is based in the correct evaluation, administration and control of risks, together with the use of authentication and encryption mechanisms such as WEP, WAP, VPN, 802.1x, among others. These they offer us different protection levels and their good operation depends in the way in that they are used inside the structured system of security.

Keywords

Information Security, Networks Security, Wireless Networks, Authentication and Encryption Mechanisms.

Tabla de Contenido

En la era tecnológica en que se vive hoy, existe en general una dependencia cada vez mayor de las redes informáticas, dada su amplia variedad de servicios y facilidades, por lo que un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones en una organización.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y técnicas utilizadas para violentar los sistemas de información y las redes en las que funcionan, cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización, debido a la falta de planificación estratégica a la hora de realizar un proyecto en el área de tecnologías de información. Además, es válido hacer referencia a las deficiencias de algunos tipos de hardware y software, que sin intención alguna muestran vacíos a nivel de seguridad.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y la propiedad de recursos y sistemas. *"Hackers"* y *"crakers"*, entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes.

Conociendo la problemática actual, es que nace el proyecto de realización de un artículo de carácter investigativo, empírico y bibliográfico, el cual presente las tecnologías existentes para mejorar el nivel de seguridad en redes inalámbricas, no sin antes, ofrecer al lector los conocimientos básicos relacionados con las redes de comunicación de datos, voz y video, que se utilizan en la actualidad. Además, procura mostrar las aplicaciones vigentes y futuras del mercado y las tendencias de las mismas, haciendo énfasis especialmente en nuevas soluciones empresariales propuestas por los grandes productores de hardware y software relacionados con la seguridad informática para redes inalámbricas.

Antecedentes históricos de las redes inalámbricas.

El arte de la comunicación es tan antiguo como la humanidad. En la antigüedad se hacia uso de tambores y humo para transmitir información entre localidades. A medida que paso el tiempo se crearon otras técnicas, hasta que en 1834 con la invención del telégrafo y el uso del código Morse se inicia la era de la comunicación electrónica, en donde destaca la invención del teléfono.

Posteriormente, finalizada la Segunda Guerra Mundial, surgen las computadoras y con ellas la necesidad de comunicación entre las mismas, dando origen después a las redes de computadoras, sus estándares, topologías y servicios. Entre ellas, se destacan las redes inalámbricas, como base de nuestra investigación, y es así, que en 1887 Heinrich Rudolph Hertz, un físico alemán, demostró que existían las ondas electromagnéticas y que éstas podrían ser usadas para mover información a muy grandes distancias. Las bases teóricas de las ondas electromagnéticas fueron desarrolladas mucho antes por el físico escocés James Clerk Maxwell en 1864. El primer uso de las ondas electromagnéticas fue la telegrafía inalámbrica. Este relevante acontecimiento sería el predecesor de la propagación electromagnética o transmisión de radio.

Utilizando estos conceptos, el italiano Guglielmo Marconi inventa la radio en 1901. La radio fue el primer medio masivo de comunicación inalámbrica y a poco más de 100 años de su invención, las comunicaciones móviles han demostrado ser una alternativa a las redes cableadas para ofrecer nuevos servicios que requieren gran ancho de banda, pero con otros beneficios como la movilidad y la ubicuidad, estar comunicado en cualquier lugar, en cualquier momento.

Las primeras redes móviles

En los 1920s, nacen las primeras redes de comunicación móvil. Eran sistemas de radio comunicación que trabajan en ese entonces a 2 MHz. El sistema se fue perfeccionando conforme transcurrían los años hasta que en los 1950s se establecieron las primeras dos bandas tal y como las conocemos ahora; la banda de VHF de radio de 150 MHz y la banda de UHF de radio en los 450 MHz.

En 1973 Martin Cooper introduce el primer radioteléfono mientras trabajaba para la compañía Motorola, Cooper pionero en esta tecnología, se le considera como "el padre de la telefonía celular". En 1979 aparece el primer sistema comercial en Tokio Japón por la compañía NTT (Nippon Telegraph & Telephone Corp.) dos años más tarde en Estados Unidos surge también el primer sistema celular analógico comercial que trabajaba en la banda de los 800 MHz. En otros países ocurrió lo mismo y surgieron muchas tecnologías paralelas pero incompatibles entre sí.

Los grandes avances en la telefonía celular digital y la amplia gama de servicios que se pueden ofrecer sobre la plataforma digital, han permitido el desarrollo de la industria de las Redes Inalámbricas como las WLANs (Wi-Fi), WPANs y WWANs.

Redes de Computadoras

Las redes de computadoras se conceptualizan como un conjunto de computadoras interconectadas entre sí, con el propósito de intercambiar información y compartir recursos (impresoras, scanner, discos duros, etc.).

Las redes se pueden clasificar según las dimensiones de la tecnología de transmisión y del tamaño.

Por tecnología de transmisión:

- **Broadcast:** Un solo canal de comunicación compartido por todas las máquinas. Un paquete enviado por alguna máquina es recibido por todas las otras.
- **Point-to-point:** Muchas conexiones entre pares individuales de máquinas. Los paquetes de X a Y pueden atravesar máquinas intermedias, entonces se necesita el ruteo (routing) para dirigirlos.

Por escala:

- **Redes de área local (LAN):** Son redes de propiedad privada que permite la conexión de clientes que se encuentran físicamente a distancias cortas. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo, compartir recursos e intercambiar información. Suelen usar una tecnología de transmisión que consiste en un cable sencillo al cual están conectadas todas las máquinas. Pueden tener diversas

topologías, entre ellas: de bus y de anillo. Las LANs tradicionales se ejecutan a una velocidad de 10 a 100 Mbps, tiene baja latencia y baja tasa de errores. Mientras, las más nuevas funcionan hasta a 10 Gbps. Dentro de este tipo de red podemos nombrar a INTRANET, una red privada que utiliza herramientas tipo Internet, pero disponible solamente dentro de la organización. Ej: IEEE 802.3 (Ethernet), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring)

- **Redes de área metropolitana (MAN):** Es una versión de mayor tamaño de la red local. Puede ser pública o privada. Una MAN puede soportar tanto voz como datos. Una MAN tiene uno o dos cables y no tiene elementos de intercambio de paquetes o conmutadores, lo cual simplifica bastante el diseño. La razón principal para distinguirla de otro tipo de redes, es que para las MAN's se ha adoptado un estándar llamado DQDB (Distributed Queue Dual Bus) o IEEE 802.6. El principal y más conocido ejemplo de una MAN es la red de televisión por cable.
- **Redes de área amplia (WAN):** Son redes que abarcan una gran región geográfica, con frecuencia un país o un continente. Este tipo de redes contiene un conjunto de máquinas diseñado para programas (es decir aplicaciones) de usuario llamadas hosts o sistemas finales (end system). Los sistemas finales están conectados a una subred de comunicaciones. La función de la subred es transportar los mensajes de un host a otro. En la mayoría de las redes de amplia cobertura se pueden distinguir dos componentes: Las líneas de transmisión y los elementos de intercambio (conmutación). Las líneas de transmisión se conocen como circuitos, canales o troncales. Los elementos de intercambio son computadores especializados utilizados para conectar dos o más líneas de transmisión. Las redes de área local son diseñadas de tal forma que tienen topologías simétricas, mientras que las redes de amplia cobertura tienen topología irregular. Otra forma de lograr una red de amplia cobertura es a través de satélite o sistemas de radio. Ej. : X.25, RTC, ISDN, etc.

Redes Inalámbricas

Como primera aproximación, las redes inalámbricas se pueden dividir en tres categorías principales:

- Interconexión de sistemas: se refiere a la interconexión de componentes de una computadora que utiliza radio de corto alcance. Estas redes utilizan el paradigma del maestro y el esclavo.
- LAN´s Inalámbricas: son sistemas en los que cada computadora tiene un módem de radio y una antena mediante los que se puede comunicar con otros sistemas. Funcionan dentro del estándar 802.11, que la mayoría de los sistemas implementa y que se ha extendido ampliamente.
- WAN´s Inalámbricas. son redes con alto ancho de banda, y su enfoque inicial es el acceso inalámbrico a Internet. Se desarrollan según el estándar 802.16.

En cuanto a las ventajas que presenta esta tecnología en comparación con las redes alámbricas, se tiene una mayor comodidad, productividad y costos. (Ver tabla 1).

- **Movilidad:** Las redes inalámbricas pueden proveer a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red alámbrica.
- **Simplicidad y rapidez en la instalación:** La instalación de una red inalámbrica puede ser tan rápida y fácil y además que puede eliminar la posibilidad de tirar cable a través de paredes y techos.
- **Flexibilidad en la instalación:** La tecnología inalámbrica permite a la red ir donde la alámbrica no puede ir.
- **Costo de propiedad reducido:** Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN alámbrica, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

- **Escalabilidad:** Los sistemas de WLANs pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

Desgraciadamente, una desventaja notable es que a mayor velocidad de transmisión, menor área de cobertura de la señal y viceversa. Además, posibles problemas de cobertura, menos velocidad, seguridad

Tabla 1:
Comparación de las ventajas e inconvenientes entre redes alámbricas e inalámbricas

Tecnología de Red	Ventajas	Desventajas
Redes Cableadas	Tecnología consolidada al 100%. Altas velocidades de transmisión. Confiabilidad. Cumplimiento de varios estándares.	Reparaciones costosas. Tiempo medio entre fallos es menor y el tiempo de reparación es mayor. Dificultad para el tendido del cableado o la reutilización de este. Tiempo de instalación.
Redes Inalámbricas	Buenas características de desempeño Bajo coste de operación. Facilidad de instalación. Facilidad de mantenimiento y detección de fallos. Fácil integración con redes existentes	Potencia y distancia limitadas. Velocidad de transmisión limitada. Tecnología aún no consolidada al 100%.

Fuente: Elaborado por el autor.

Topologías o configuraciones básicas

Una red *Ad-hoc*, también conocida como IBSS (Independent Basic Service Set), es una red simple donde se establecen comunicaciones entre las múltiples estaciones en un área de cobertura dada sin el uso de un punto de acceso o servidor. La norma especifica la etiqueta que cada estación debe observar para que todas ellas tengan un acceso justo a los medios de comunicación inalámbricos. Proporciona métodos de petición de arbitraje para utilizar el medio para asegurarse de que el rendimiento se maximiza para todos los usuarios del conjunto de servicios base.

Las redes cliente/servidor utilizan un punto de acceso que controla la asignación del tiempo de transmisión para todas las estaciones y permite que estaciones móviles deambulen por la

columna vertebral de la red cliente / servidor. El punto de acceso se usa para manejar el tráfico desde la radio móvil hasta las redes cliente / servidor cableadas o inalámbricas. Esta configuración permite coordinación puntual de todas las estaciones en el área de servicios base y asegura un manejo apropiado del tráfico de datos. El punto de acceso dirige datos entre las estaciones y otras estaciones inalámbricas y/o el servidor de la red. Típicamente las WLAN controladas por un punto de acceso central proporcionara un rendimiento mucho mayor.

Los estándares de WLAN

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso de IEEE (Institute of Electrical and Electronics Engineers) y ETSI (European Telecommunications Standards Institute). Una vez desarrollados se convierten en la base de los fabricantes para desarrollar sus productos.

Entre los principales estándares se encuentran:

- IEEE 802.11: El estándar original de WLANs que soporta velocidades entre 1 y 2 Mbps.
- IEEE 802.11a: El estándar de alta velocidad que soporta velocidades de hasta 54 Mbps en la banda de 5 GHz.
- IEEE 802.11b: El estándar dominante de WLAN (conocido también como Wi-Fi) que soporta velocidades de hasta 11 Mbps en la banda de 2.4 GHz.
- HiperLAN: es un sistema de radiocomunicación de corto alcance al margen de IEEE 802.11, pero que utiliza esta norma como borrador y la tecnología spread spectrum en el rango de frecuencias de los 2.4Ghz.
- HiperLAN2: Estándar que compite con IEEE 802.11a al soportar velocidades de hasta 54 Mbps en la banda de 5 GHz.
- HomeRF: Estándar que compite con el IEEE 802.11b que soporta velocidades de hasta 10 Mbps en la banda de 2.4 GHz.

Tabla 2:
Principales estándares WLAN

Estándar	Velocidad máx.	Interfase	Bandwidth	**Frecuencia**
802.11b	11 Mbps	DSSS	25 MHz	2.4 GHz
802.11a	54 Mbps	OFDM	25 MHz	5.0 GHz
802.11g	54 Mbps	OFDM/DSSS	25 MHz	2.4 GHz
HomeRF2	10 Mbps	FHSS	5 MHz	2.4 GHz
HiperLAN2	54 Mbps	OFDM	25 MHz	5.0 GHz
5-UP	108 Mbps	OFDM	50 MHz	5.0 GHz

Fuente: Eveliux.com

Seguridad en redes inalámbricas

¿Son las redes inalámbricas seguras? Esta parece ser la mayor interrogante que se presenta con respecto a las redes inalámbricas, hoy en día, si bien es de conocimiento general las grandes ventajas con que se cuenta al implementar esta tecnología, también lo es, que dada la naturaleza de la transmisión por RF y sus riesgos intrínsecos, es necesario tomar medidas adicionales de seguridad para las WLANs.

Aunque, claro esta, no existen las redes “seguras”, si existen políticas, dispositivos y mecanismos que nos brindan diferentes niveles de seguridad, y que, si se instauran de manera adecuada, nos permite reducir los posibles riesgos a los que se expone una organización que opte por el uso de las tecnologías de comunicación sin cables.

Políticas y Mecanismos de Seguridad

Las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

Las PSI conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. En razón de lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos. Las PSI constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben

constituir un proceso continuo y retroalimentado que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y la renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

Un mecanismo de seguridad es aquel que se encarga de proveer una serie de servicios dentro de la red, en este caso nos referimos a los relacionados con el área de seguridad; para lograr su fin, estos mecanismos utilizan como común denominador técnicas de encriptación y autenticación, y necesitan para su mejor funcionamiento, ser implementados en orden. La calidad en sus servicios puede variar según la implementación de los mismos.

Las técnicas de encriptación constan de un proceso algorítmico lógico y matemático, por medio del cual la información es codificada, con el fin de garantizar su integridad, mientras los mecanismos de autenticación son procesos de identificación de un equipo o usuario. Dentro de la variedad de mecanismos de autenticación es importante hacer referencia a los siguientes: SSID, MAC Address, OSA, ACL y CNAC.

Tabla 3:
Evolución de la Seguridad para redes inalámbricas

Evolución de la seguridad WLAN

Ante las carencias de WEP, WPA surge como el "enlace" con el futuro 802.11i

	Wired Equivalent Privacy	Wi-Fi Protected Access	802.11i o Wi-Fi Protected Access Version 2
Acrónimo	WEP	WPA	WPA2
Características	Claves de encriptación basadas en el algoritmo RC4 (típicamente claves de 40 bits).	Claves estáticas que facilitan los ataques de los hackers Añade TKIP (Temporal Key Integrity Protocol), que aporta rotación de claves y refuerza la encriptación.	Fuerte encriptación AES basada en el algoritmo Rijndael (claves de 128, 192 ó 256 bits). Añade dos potentes características de autenticación: Wireless Robust Authentication Protocol (WRAP) y Counter With Cipher Block Chaining Message Authentication Code Protocol (CCMP).
Ciclo de vida	1997-2003	2003-2004	2004-????

Fuente: Comunicaciones World

El SSID consta de un conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos inalámbricos se puedan comunicar, deben tener

configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red inalámbrica en los que viaja en texto claro, no puede ser tomado como una medida de seguridad.

Otra alternativa, es la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo. Es un mecanismo robusto pero vulnerable para expertos que sepan suplantar en un dispositivo de red una determinada dirección MAC autorizada, aunque es necesario conocer dicha dirección MAC.

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

Con respecto a Open System Autentication (OSA), es definido por el estándar 802.11 para autentificar todas las peticiones que recibe, pero presenta como su principal problema, que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aun activando WEP, por lo tanto es un mecanismo poco fiable. EL ACL (Access Control List) tiene la gran ventaja que es soportado por la mayoría de los productos comerciales. Utiliza, como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la lista de control de acceso. CNAC (Closer Network Access Control) es otro mecanismo, el cual pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando este como contraseña.

WEP (Wired Equivalent Privacy).

Es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11, protege los datos a nivel de enlace de las transmisiones inalámbricas y se basa en el algoritmo RC4. Tiene como sus objetivos: proporcionar confidencialidad, autentificación y control de acceso en redes inalámbricas. WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso, la cual debe ser escrita de manera manual, pues el estándar no contempla

ningún mecanismo de distribución automática de claves, generando así varios inconvenientes, tales como: aumento de posibilidades de que la clave sea comprometida, y provoca un aumento de mantenimiento por parte del administrador de la red.

Se ha demostrado que WEP adolece problemas en cuanto al nivel de seguridad ofrecido, la mayoría de ellos relacionado con el vector de inicialización y la forma de utilizar el algoritmo RC4. Entre los objetivos de WEP, se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes, sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje. Con respecto al mecanismo de autentificación, WEP no incluye autentificación de usuarios, sino la autentificación de estaciones que dentro de su configuración tenga almacenada la clave. El sistema de autentificación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante.

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica. Debido a esta problemática surge en el mercado, otras alternativas para poder implementar una red inalámbrica con niveles de seguridad mas óptimos, tal es el caso de la tecnología de VPNs, la cual está suficientemente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperatibilidad entre dispositivos de distintos fabricantes. Además, WAP y WAP2, que son mecanismos diseñados específicamente para redes WLAN que se considera son los sucesores de WEP.

WAP (Wi-Fi Protected Access)

Fue desarrollado por la WECA para solucionar todas las debilidades conocidas de WEP y se considera suficientemente seguro. Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación. Este protocolo toma como base el borrador de la norma 802.11i, y adopta la norma 802.1x para la autentificación de usuarios mediante el uso de un servidor RADIUS, donde se almacenan las credenciales y contraseñas de los usuarios de la red inalámbrica. Para no obligar al uso

de tal servidor para el despliegue de redes inalámbrica, WPA permite la autentificación mediante clave compartida (PSK, Preshared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

La principal ventaja del WPA frente al WEP es que emplea un algoritmo de claves temporales utilizado para autenticar conocido como TKIP (Temporal Key Integrity Protocol), el mismo, ofrece un mecanismo automático de renovación de claves para cada paquete, por lo que se impide reproducir el ataque con el WEP, dado que no se puede recoger la suficiente información encriptada bajo la misma clave. Añade un campo de MIC (Message Integrity Check, control de la integridad del mensaje) al paquete, y utiliza 802.1X. Sus principales características son la renovación automática de la clave de encriptación de los mensajes y un vector de inicialización de 48 bits. TKIP fue diseñado por los mejores criptógrafos y ofrece un recubrimiento alrededor de WEP, cerrando los hoyos de seguridad de la misma.

Por otro lado, contamos con los servicios de autenticación ofrecidos por 802.1x, para poder controlar el acceso directamente en el puerto de acceso. Al insertar el estándar 802.1x la autentificación de usuario se llevará a cabo directamente en el área de acceso a la red. Los derechos y programas propios de cada usuario no le serán asignados, es decir no tendrán acceso a ellos, hasta que se haya hecho una autentificación satisfactoria.

El sistema está formado por tres componentes primarios:

- el cliente (Supplicant), que se quiere autentificar, para conseguir el acceso a la red.
- el AP (Authenticator), que se encarga de habilitar el puerto tras autenticar el cliente por medio del servidor de autenticación.
- EL servidor de autenticación (Authenticaton Server), que incluye los datos del usuario y comprueba si el cliente está autorizado para acceder a la red.

EAP (Protocolo de Autenticación Extensible) es otra tecnología que emplea WAP y prácticamente es un protocolo punto a punto que proporciona un mecanismo para soportar métodos de autenticación múltiples, entre los que se incluyen tarjetas de identificación, Kerbeos, RADIUS (Remote Dial-In User Service), contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros.

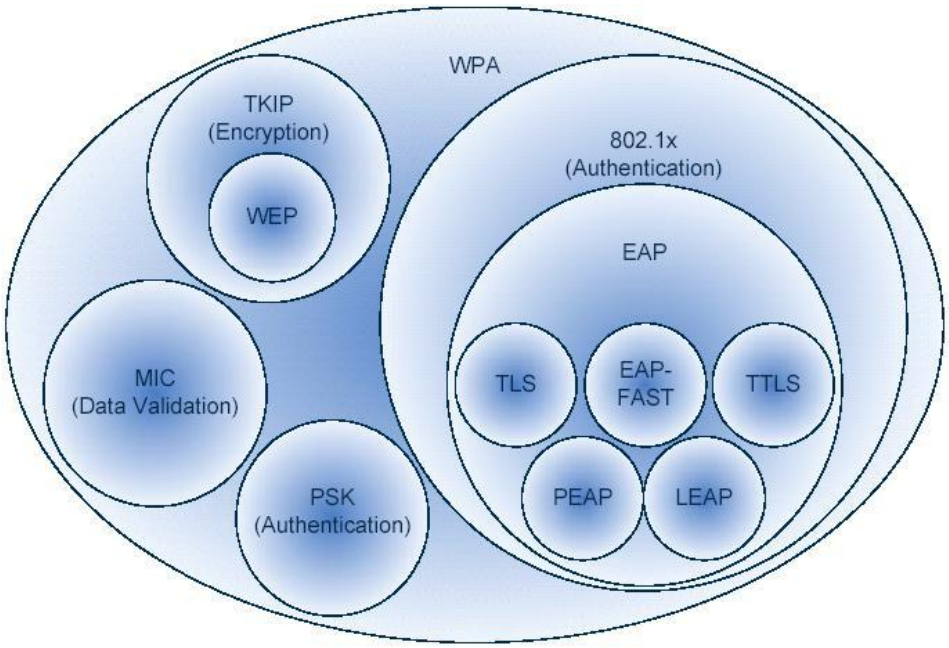
Cuando una red inalámbrica utiliza EAP, y existe una nueva petición de conexión por parte de un nuevo dispositivo móvil sobre un punto de acceso. Antes de realizarse la autenticación por parte del punto de acceso, el punto de acceso pregunta a un servidor de autenticación como RADIUS, por la veracidad de este.

Una vez el servidor ha comprobado la veracidad del nuevo dispositivo móvil, manda su respuesta al punto de acceso, y este concluye la autenticación del nuevo dispositivo móvil si la respuesta por parte del servidor de autenticación ha sido satisfactoria.

De este modo, los puntos de acceso que implementa EAP no necesitan implementar un método concreto de autenticación, actúan como simples pasarelas entre el dispositivo móvil y un servidor de autenticación que puede utilizar varios métodos de autenticación.

Existen multitud de métodos EAP especificados (alrededor de 40), siendo los más comunes en la actualidad los siguientes: EAP-TLS, EAP-TTLS, PEAP.

Figura 1:
WAP: Protocolos y mecanismos integrados, todo en uno.



Fuente: LXE Inc.

No obstante, el buen funcionamiento y calidad de servicio para seguridad ofrecidos por WAP, surgen nuevos retos en cuanto al área de estudio, es así que se da origen a WPA2

(IEEE 802.11i), este nuevo estándar del IEEE para proporcionar seguridad en redes inalámbricas, incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Además, 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.

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

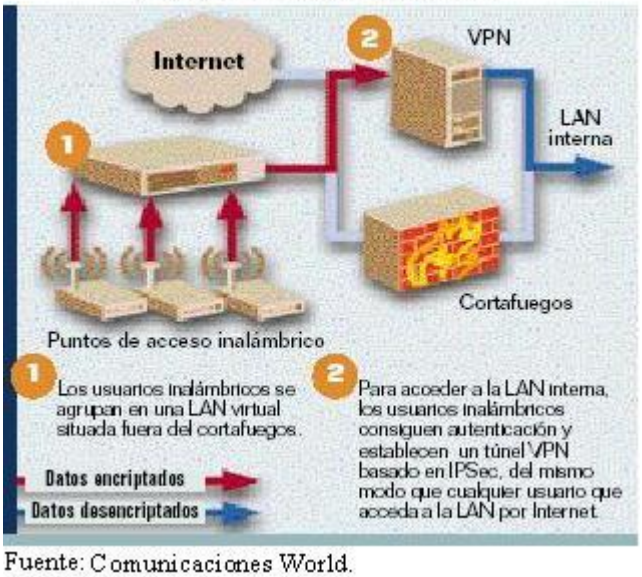
VPN

Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

Existe un gran número de protocolos de túnel. Los más importantes son el L2TP (Layer 2 Tunneling Protocol, Protocolo de Túnel de capa 2) y el IPSec (IP Security Protocol, Protocolo de Seguridad IP).

- **L2TP:** El IETF (Grupo de Trabajo de Ingeniería de Internet) ha desarrollado el protocolo L2TP que es una combinación del protocolo PPTP y del protocolo L2F (Layer 2 Forwarding) desarrollado por Cisco, el L2TP combina las ventajas de los protocolos que lo forman. El protocolo L2TP en Windows ya no utiliza el MPPE (Microsoft Point-to- Point Encryption, Protocolo de encriptación de punto a punto de Microsoft), cuando utiliza

Figura 2
IPSec en entornos inalámbricos



Fuente: Comunicaciones World.

el IPSec. Es decir, que en las conexiones VPN basadas en L2TP se usa una combinación de L2TP y una IPSec. También son posibles los protocolos IP, IPX (Internet Work Packet Exchange, Intercambio de paquetes de Internet), etc.

- **IPSec:** El protocolo consta de dos partes, una parte se encarga de la codificación de los datos y la otra parte de asegurar su integridad y autenticidad. El primer componente de la IPSec es ESP (Carga de Seguridad Encapsulada) que se encarga de la codificación, para la que se pueden emplear distintos procedimientos de encriptación. El segundo componente se denomina AH (Cabecera de autentificación) que impide la manipulación de los datos. El protocolo IKE (Intercambio de claves de internet) no es un componente de las IPSec; sin embargo, está estrechamente vinculado a él, es el encargado de la gestión de claves. IPSec ha demostrado ser un protocolo seguro; hasta la fecha no ha podido ser pirateado.

Tabla 4:
Pros y contras de la seguridad inalámbrica

	802.1x	Basada en navegador	IPSec	WEP
Pros	Satisface mejor os requerimientos de seguridad. Refuerza la autenticación y la encriptación a nivel de enlace, soportando todos los protocolos. Bajo overhead.	Mayor compatibilidad con dispositivos inalámbricos con navegador. Fácil de usar por usuarios invitados y visitantes.	El mayor modelo de seguridad disponible; puede usar certificados digitales o autenticación de dos factores. Generalmente disponible para plataformas informáticas. Puede emplearse con infraestructuras VPN (para teletrabajo, por ejemplo).	Amplio soporte para encriptación de 64 y 128 bits Configuración sencilla Encriptación integrada en las tarjetas inalámbricas.
Contras	Los usuarios no Windows precisan comprar e instalar el cliente, que no está preparado aún para todas las paltaformas. No lo soportan todos los puntos de acceso. Los servidores RADIUS compatibles con EAP de 802.1x precisan permisos y denagaciones de acceso.	No funciona con dispositivos embebidos. No proporciona encriptación. El tráfico puede ser fácilmente "fisgoneado" en entornos cableados e inalámbricos; no protege las conexiones de inalámbrico a inalámbrico.	Configuración y distribución de políticas compleja, especialmente a través de plataformas y fabricantes. El rendimiento a velocidades LAN puede ser problemática para laptops; los gateways de seguridad BPM centrales podrían necesitar ser actualizados. Soporte sólo IP; no soporta multimedia IP; no protege las conexiones de inalámbrico a inalámbrico.	Muchos problemas potenciales de seguridad. Las claves WEP se conocen y comparten ampliamente. No proporciona autenticación entre usuario final y sistema final.

Fuente: Comunicaciones World

Recomendaciones de seguridad para la implementación de una red inalámbrica

A estas alturas, es de conocimiento general la problemática que presentan las redes inalámbricas en cuanto a seguridad se refieren, sin embargo el talón de Aquiles de estas redes puede encontrar su solución. No obstante que, por muy singulares que los problemas de redes inalámbricas puedan parecer, muchos se pueden encarar mediante procedimientos de seguridad convencionales y tecnologías de seguridad, mismas que deben ser aplicadas por capas y como complemento una de la otra, hay que tener siempre presente que estas medidas deben aplicarse en primer lugar según las vulnerabilidades internas de la empresa, pues es aquí donde se origina el mayor índice de riesgos, posteriormente se debe tomar medidas para contrarrestar los riesgos originados por factores externos.

Este tema es tan amplio que inclusive existe en el mercado una variedad de soluciones empresariales ofrecidas por grandes compañías involucradas en la producción de hardware y software para tecnologías inalámbricas, tal es el caso de Cisco Systems, Alcatel, 3Com, Microsoft, y otra más.

Para poder considerar una red inalámbrica como segura, debería cumplir una serie de requisitos elementales, tales como:

- Confinar las ondas de radio tanto como sea posible. Mediante el uso de antenas direccionales y configurando adecuadamente la potencia de transmisión de los AP.
- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Para lograr alcanzar estos requisitos, se debe seguir un plan estratégico y metódico, que permita evaluar los riesgos actuales y a futuro, implementando los debidos controles para cada uno de los riesgos. Además, diseñar una estructura de aplicación práctica de los principios de seguridad por capas, basada en mecanismos de autenticación y encriptación, que favorezca la confiabilidad e integridad de la red.

Estos principios deben ser aplicados de acuerdo a 3 enfoques que se le da a la seguridad:

Seguridad Física

Es de suma importancia efectuar un reconocimiento del entorno físico, evaluar la transmisión y la cobertura de radio para reducir el riesgo de descubrir su emisión, realizar una auditoria de la red inalámbrica para identificar posibles vulnerabilidades y eliminar puntos en la topología en los cuales el tráfico broadcast sea innecesario.

Seguridad de la Infraestructura

- Hacer un inventario de las direcciones MAC negando el acceso a sus AP a aquellas direcciones MAC que no estén inventariadas.
- Hacer uso de direcciones estaticas o la asignación de direcciones IP ligadas a las listas de control de acceso MAC en sus AP. El uso de DHCP debe de evitarse, pero en caso contrario el mismo debe ser implementado en conjunto alguna medida de autenticación.
- Los SSIDs para los AP y clientes deben ser largos y difíciles de adivinar.
- Como mínimo se debe activar WEP como método de control de acceso.

Seguridad de la Administración de la Infraestructura

- Aplique todas las medidas disponibles a sus AP para asegurarlos frente a accesos no autorizados, por ejemplo podría desactivar accesos SNMP/Telnet, configurar contraseñas seguras y controles de acceso.

Otras recomendaciones, que es importante tomar en cuenta a la hora de implementar redes de tecnología inalámbrica:

- Aislar la red inalámbrica de la red cableada, la mejor forma de conseguirlo es implementar un protocolo VPN con encriptación fuerte como por ejemplo IPSec, y no permitir el tráfico en ningún otro protocolo.
- Ubicación de puntos de acceso en redes DMZ (para mitigar cualquier intrusión).
- Utilizar VPNs en la comunicación con los usuarios (para proteger el contenido de las transmisiones y poder contar con el sistema de autentificación del servidor de VPNs).

- Autentificar el acceso de los usuarios a través de la red inalámbrica con un servidor de autentificación. Por ejemplo, el estándar 802.1x soporta nuevos tipos de autentificación para integraciones con servidores RADIUS.
- Utilizar un mecanismo de autentificación fuerte protegido mediante encriptación, para impedir los accesos no autorizados, por ejemplo, TLS, PEAP o TTLS.
- Auditar y escanear la red inalámbrica, haciendo uso de detectores de redes y herramientas de escaneo.
- Es imperativo tratar a toda red inalámbrica, por muchas medidas de seguridad que tenga, como una red insegura. Una práctica muy recomendada es tratarlas como redes DMZ, y conectar los diferentes puntos de acceso a una red DMZ independiente que a su vez está conectada al firewall corporativo. De esta forma se puede regular exactamente que tipos de tráfico y que recursos de la red interna son accedidos desde la red inalámbrica.

Soluciones Empresariales para el diseño de seguridad en una red inalámbrica

La mayor productora de software a nivel mundial, se ha dado a la tarea de ampliar y optimizar los servicios ofrecidos a miles de clientes en el área de redes inalámbricas, por lo que ha investigado y lanzado al mercado soluciones empresariales para el uso de esta tecnología. *Servicios de Certificate Server de Microsoft Windows Server 2003* y *Seguridad en LAN inalámbricas con PEAP y contraseñas*, son dos soluciones que le guían a través del ciclo completo de planeamiento, implementación, prueba y administración de soluciones de seguridad inalámbricas.

La primera de ellas utiliza certificados digitales para la autenticación del acceso de usuarios y equipos de red, mientras la segunda, utiliza nombres de usuario y contraseñas.

El uso de estas soluciones conlleva la utilización de mecanismos de autenticación y encriptación como. WAP, EAP, VPN, IPSec, Servidores RADIUS, Aunque claro esta que la principal recomendación de Microsoft es el uso de los mecanismos de seguridad ofrecidos por 802.1x.

Tabla 5.
Comparación de los enfoques de seguridad de WLAN

Característica	WLAN 802.1X	WEP estática	VPN	IPSec
Autenticación Segura	Sí	No	Sí, pero no las VPN que utilicen autenticación de clave compartida.	Sí, si se emplea autenticación de certificados o Kerberos.
Cifrado de datos de alta seguridad	Sí	No	Sí	Sí
Conexión transparente y reconexión a la WLAN	Sí	Sí	No	Sí
Autenticación de usuario	Sí	No	Sí	Sí
Autenticación de equipo	Sí	Sí	No	Sí
Difusión y tráfico de multidifusión protegidos	Sí	Sí	Sí	No
Se requieren dispositivos de red adicionales	Servidores RADIUS	No	Servidores VPN, servidores RADIUS	No
Acceso seguro a la propia WLAN	Sí	Sí	No	No

Fuente: Microsoft

Por otra parte, Cisco proyecta en el mercado el uso de la solución Cisco Wireless Security Suite, un estándar empresarial en cuanto a seguridad inalámbrica se refiere, en especial para el uso con los productos inalámbricos Cisco Aironet. Esta solución proporciona servicios de seguridad inalámbricos robustos que ofrecen libertad y movilidad a los usuarios finales de la red mientras provee un ambiente seguro.

Prácticamente su funcionamiento utiliza una estructura de mecanismos de autenticación y encriptación, aplicados de manera que ofrezca cada uno un nivel de seguridad complementario a los demás.

Las garantías de seguridad obtenidas mediante el uso de CWSS se deben a que ofrece soporte para 802.11i y la autenticación mediante Servidores RADIUS o Servidores AAA, soporta los diferentes tipos de EAP (Cisco LEAP, EAP-FAST, EAP-TLS, PEAP, EAP-TTLS, EAP-SIM). Además, soporta certificaciones de seguridad mediante WPA y WPA2, y los diferentes tipos de autenticación en 802.1x, y finalmente utiliza TKIP, WEP y AES para la encriptación de datos.

Conclusión

La seguridad informática en redes de computadoras es un factor de suma importancia, el cual requiere de una correcta evaluación, administración y control de riesgos, ya sean internos o externos; y para comprenderla habría que despejarse una gran serie de interrogantes en cuanto a nuestro estado físico y tecnológico actual.

Es una realidad que las tendencias a violentar los sistemas tecnológicos de información tanto en hardware como software crecen con el pasar del tiempo, sin embargo los ataques informáticos a redes de computadoras se reducen debido a las ventajas obtenidas por diferentes mecanismos de autenticación y encriptación, aún así, no se debe confiar plenamente en una estructura de seguridad definida y establecida, pues hoy puede brindar un gran nivel de confiabilidad, pero mañana, es otro día, y en un entorno tecnológico innovador y cambiante nace la interrogante ¿Estamos preparados para lo que viene?. Hay que tener presente que las amenazas son cosas que no podemos controlar porque son externas, lo único que podemos controlar es nuestras vulnerabilidades y activos. Sin duda alguna, las herramientas existentes en la actualidad son muy útiles y talvez indispensables, pero lo que realmente importa es como se administre todo eso para que junto con las políticas y procedimientos apropiados se logre un entorno seguro.

Referencias

3Com Corporation. (2001). Technical Brief: *Comparing Performance of 802.11b and 802.11a Wireless Technologies*. 3Com Corporation.
www.3com.com

3Com Corporation. (2003). *Deploying 802.11 Wireless LANs*. 3Com Corporation.
www.3com.com

Cisco Systems, Inc. (2002). *A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite*. Cisco Systems, Inc..
www.cisco.com

Cisco Systems, Inc. (2004). *Deployment Guide: Configuring the Cisco Wireless Security Suite*. Cisco Systems, Inc.
www.cisco.com

Cisco Systems, Inc. (2005). *Cisco Wireless Security Suite*. Cisco Systems, Inc.
www.cisco.com

Comunicaciones World. (2001). *Encriptación y Autenticación: Seguridad en el aire*. Revista Comunicaciones World.
www.idg.es/comunicaciones/index.asp

Convery, S y Millar, D. (2003). *Cisco SAFE: Wireless LAN Security in Depth*. San Jose, CA: Cisco Systems, Inc.
www.cisco.com

Ekström, D.(2003). *Securing a wireless local area network - using standard security techniques*. Tesis de Maestria en Ingeniería de Software no publicada, Blekinge Institute of Technology, Suecia.

Enterasys Networks. (2001). *RoamAbout: 802.11 Wireless Networking Guide.* Rochester, NH: Enterasys Networks.

Flikenger, R. (2002). *Building Wireless Security Networks*. O´Reilly.

García, F. (2003). *Seguridad y multiplicidad de estándares: Retos de las tecnologías inalámbricas*..

LXE, Inc. (2003). *RF/Wireless Basics "An Intro to Wireless Data Collection Networks, Products, Standards and Solutions"*. LXE, Inc.
www.lxe.com

LXE Inc. (2004). *The New 'Keeping the Bad Guys Out of Your for 802.11 Wireless Data Collection Network.* LXE Inc.
www.lxe.com

Microsoft (2004). *Microsoft Solutions for Security: Securing Wireless LANs with Certificate Services*. Microsoft TechNet.

Microsoft. (2004). *Microsoft Solutions for Security: Securing Wireless LANs with PEAP and Passwords*. Microsoft TechNet.

Ouellet, E. y Padjen, R. (2002). *Building a Cisco Wireless LAN.* Rockland, MA: Syngress Publishing Inc.

Tanenbaum, A. (2003). *Redes de Computadoras*. 4ta. Edición. México: Pearson and Prentice Hall.