SEGURIDAD EN REDES INALÁMBRICAS

Ing. Henry Eliseo Navarro Chinchilla[1]

[1]Ingeniero de Sistemas, Docente de la Facultad de Ingenierías - Universidad Francisco de Paula Santander Seccional Ocaña
henavarroc@ufpso.edu.co

Abstract

Within the expectations generated by the massive use of the internet and the implementation of high- speed networks both wired and Wireless, has also proliferated violation and intrusion mechanisms penetration of networks and generating all kinds of computer crimes.

We must then take into account a number of conditions and rules to ensure the use of these networks for the least not placed at risk of intrusion of agents and outside users. We know that at present there is no computer network hundred percent sure, but the implementation of measures increasingly strong and timely permit climb this percentage close to the ideal.

This article can discover the essential elements to generate in practice security in gíreles networks that in the end are those that have shifted largely to cable networks.

Key Words

WiFi, WiMAX, Firewall, Cracking, Switch, Router, Access Point (AP), Stream cipher, VPN, Servidor Radius.

Resumen

Dentro de las expectativas que ha generado el uso masivo de internet y la implementación de redes de alta velocidad tanto cableadas como inalámbricas, ha proliferado también la violación y la intrusión como mecanismos de penetración de redes y la generación de toda clase de delitos informáticos.

Palabras Claves

Protocolo, Servidor, Encriptamiento, Servidor Radius.

SEGURIDAD EN REDES INALÁMBRICAS

Introducción

Desde los inicios de las redes inalámbricas, se ha observado que el principal problema que las aqueja es su seguridad. Tener a la mano un gran compendio de herramientas, así como establecer políticas de seguridad será lo más adecuado.

Un elemento importante es la presentación que se hace de las WiFi, que en general son las que se han estandarizado con reglas que en la actualidad las hacen más seguras, frente a las nuevas y comentadas WiMax. Para estas últimas, en los últimos meses se han dado protocolos para su operación, y hacia el futuro tendremos más y mejores elementos de seguridad para que podamos entrar a operar de una forma confiable.

Seguridad en redes inalámbricas

Los usuarios de servicios de telecomunicaciones demandan, cada día, más beneficios y flexibilidad. En los últimos años ha existido un desarrollo vertiginoso de la tecnología inalámbrica, en el campo de las redes de área local denominada WiFi y en las de área extendida denominada como WiMax.

Un aspecto de los de mayor importancia fue y es, la tendencia a que se violen todos los parámetros de seguridad de estas nuevas tecnologías, lo que ha permitido que los fabricantes de software y hardware estén todo el tiempo buscando las mejores alternativas para ofrecer a sus clientes y ganar expectativas dentro del mercado, además de buscar la unificación de estándares a través de los comités y las organizaciones encargadas de hacer valer las reglas para aplicar en conjunto.

Objetivos de seguridad

Confidencialidad: Permitir que los datos viajen seguros y solo puedan ser leídos por el destinatario. Para garantizar la confidencialidad deberemos utilizar sistemas criptográficos para que los mensajes solo puedan ser leídos por el emisor y el receptor; debemos tratar de evitar que las difusiones de RF salgan de un área mínima necesaria, para evitar el wardriving (búsqueda de redes inalámbricas) y eavesdropping (interceptación).

Integridad: No permitir que los datos que enviamos puedan ser modificados en el camino y reenviados como si fuesen nuestros.

Disponibilidad: La red debe estar disponible en todo momento y que no pueda ser atacada y desactivada. En un entorno donde las comunicaciones juegan un papel importante es necesario asegurar que la red esté siempre disponible, puesto que ahora el medio físico es el aire, es posible introducir interferencias que dejen la red fuera de servicio. Si generamos mucho ruido en la misma banda de frecuencias que se utilice en una red, esta puede dejar de funcionar o funcionar al mínimo de sus posibilidades.

Medidas mínimas para implementar seguridad

Autenticación: Es decir, un usuario ha de demostrar que es quien dice ser, cuando quiera usar la red.

Autorización: Indica qué cosas puede hacer un usuario en la red, dependiendo de su nivel de privilegios.

Contabilización: En determinados entornos, es interesante tener un servidor que almacene las operaciones que está realizando un determinado usuario, para luego investigar acciones sospechosas.

Encripción: Modifica la información transmitida utilizando un algoritmo y llaves secretas para evitar que la información sea interceptada o modificada.

Soluciones

- ✓ Política de Seguridad (Asegurar cortafuegos, software fiable, Ipsec, PKI, Proxys, Control de Acceso).
- ✓ Monitorizar y Reaccionar (Aplicaciones de sistemas de detección de intrusos-IDS).
- ✓ Comprobar escaneo de vulnerabilidades.
- ✓ Gestionar y mejorar administración de recursos (Hosts, Servidores, Routers/Switches, cifrado (protocolos seguros)).

MECANISMOS Y PROTOCOLOS DE SEGURIDAD EN REDES INALÁMBRICAS WIFI-WIMAX.

1. **SSID – Broadcast** (Service Set Identifier). Código incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. Existen algunas variantes principales del SSID. Las redes ad-hoc, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID (Basic Service Set Identifier); mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID (E de extendido). Nos podemos referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.

   Uno de los métodos más básicos de proteger una red inalámbrica es desactivar el broadcast del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo no debe ser el único método de defensa para proteger una red inalámbrica.

2. **Control de acceso por direcciones MAC.** Los dispositivos inalámbricos como los Access Point pueden restringir las direcciones MAC de las estaciones que se conecten a él. La Tabla de Direcciones MAC permitidas se define en el mismo despositivo.

3. **WEP Wired Equivalent Privacy.** Es un mecanismo de seguridad para las redes inalámbricas, mediante el cual la asociación de los dispositivos con un Access Point y la información transmitida por la red inalámbrica pueden encriptarse.

WEP utiliza el algoritmo de encripción RC4, que emplea llaves de 64, 128 o 256 bits, las cuales tienen un vector de inicialización de 24 bits. Todos los dispositivos (Estaciones y Access Point) deben tener definida unas llaves de encripción llamadas WEP Key. Estas llaves de encripción deben ser iguales en todos los dispositivos de la red inalámbrica.

Dentro de la criptografía RC4 o ARC4 es el sistema de cifrado de flujo stream cipher más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS, SSL), para proteger el tráfico de internet y WEP. RC4 fue excluido en seguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas; sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

RC4 genera un flujo pseudoaleatorio de bits (un keystream) que, para encriptación, se combina con el texto plano usando la función XOR como en cualquier Cifrado Vernam. La fase de descifrar el mensaje se realiza del mismo modo.

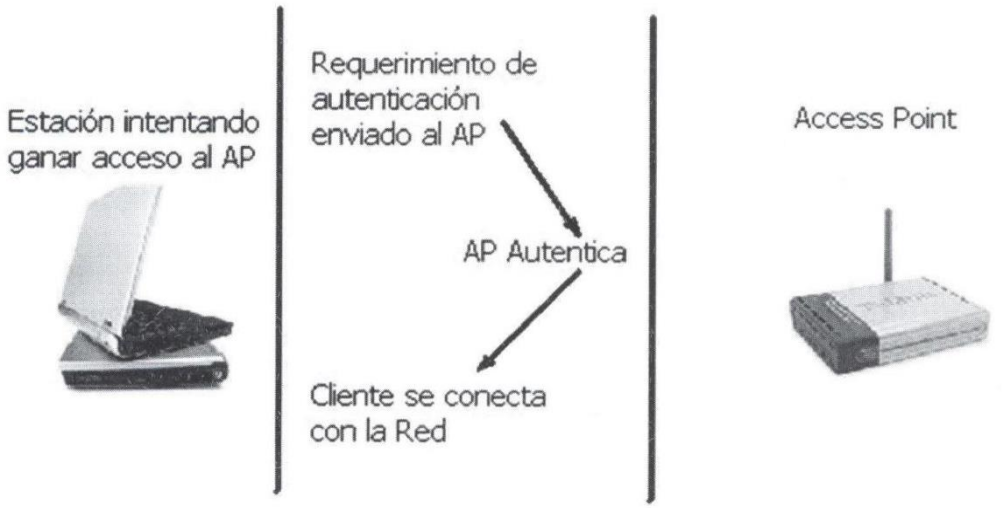
Para generar el keystream, el algoritmo de cifrado tiene un estado interno secreto que consiste en:

- ✓ Una permutación de todos los 256 posibles símbolos de un byte de longitud (lo llamaremos "S").
- ✓ Dos índices-apuntadores de 8 bits (los llamaremos "i" y "j").

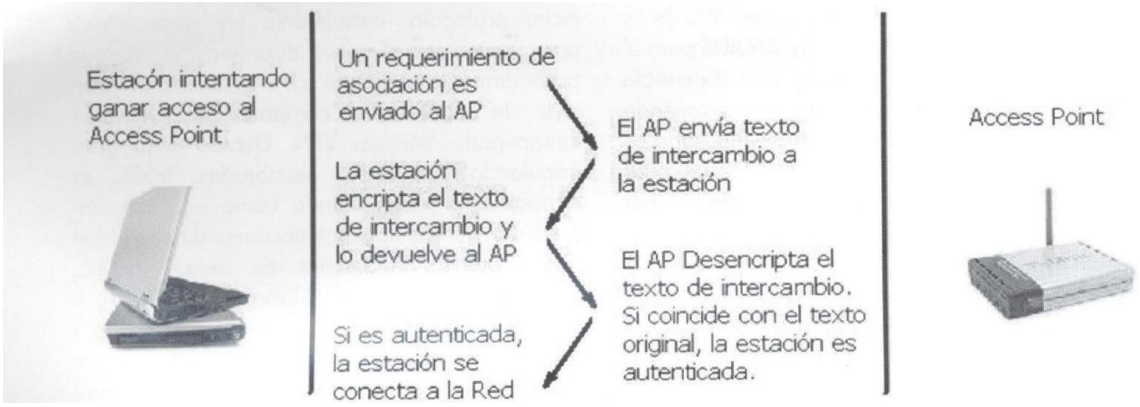
La permutación se inicializa con una clave de longitud variable, habitualmente entre 40 y 256 bits usando un algoritmo de programación de claves (Key scheduling algorithm o KSA). Una vez completado, el flujo de bits cifrados se genera usando un algoritmo de generación pseudoaleatoria (pseudo-random generation algorithm o PRGA).

WEP define 2 mecanismos para realizar la autenticación:

- ✓ **Open System.** La Autenticación Open System permite a un dispositivo asociarse con otro si coincide la información básica (SSID).



- ✓ **Shared Key.** Autenticación Shared Key; el dispositivo permite la asociación de una estación, si además del SSID, coincide la llave de encripción.



Configuración WEP de Tarjetas de Red

El mecanismo de seguridad para las redes inalámbricas se puede realizar dentro de cada una de las tarjetas de Red, dentro de su configuración, para ello hay que tener en cuenta los siguiente (Glosario de Seguridad Informática):

Encripción de Datos	:	Habilitada / Deshabilitada
Tipo de Autenticación	:	Open System \ Shared Key
Llaves de Encripción	:	Bits de Encripción. 64, 128, 256
Formato de la llave	:	ASCII o Hexadecimal
WEP Key	:	Llaves de encripción.

4. **LEAP (LightweightExtensibleAuthenticationProtocol).** Protocolo del tipo EAP patentado por Cisco, basado en el nombre de usuario y la contraseña que se envía sin protección. Esta metodología descuida la protección de las credenciales durante la fase de autenticación del usuario con el servidor. Debido a que se trata de un protocolo propietario, los fabricantes han puesto gran esfuerzo en el desarrollo y mejoras de la seguridad de los sistemas WiFi. La ventaja más obvia del protocolo LEAP es la de proveer una seria mejora a la seguridad, incorporando el concepto de una llave específica de encriptación por cada sesión; a diferencia de la encriptación estática y “Shared Key”, que están expuestas a la amenaza “WEB Cracking”. Adicionalmente, la llave es generada una vez que el acceso ha sido exitoso, la cual puede ser implementada usando una base de datos local de autenticación.

   Algunos de los beneficios del protocolo LEAP son los siguientes:

- ✓ Autenticación mejorada para los clientes wireless; utiliza una llave de encriptación por sesión.
- ✓ Administración centralizada de usuarios y llaves.
- ✓ Reducción de la exposición de la llave de encriptación. En el caso de LEAP la llave es una por sesión, a diferencia de WEP que es una para todas las sesiones.
- ✓ Permite ser implementado utilizando las bases de datos existentes para la autenticación de los usuarios.

5. **PROTOCOLO EAP (Extensible Authentication Protocol).** Otro importante modelo de seguridad para las redes WiFi es la implementación de Autenticación WLAN y administración de llaves mediante RADIUS para el protocolo EAP-TLS. El protocolo EAP (Extensible Authentication Protocol) es una estructura diseñada para la autenticación de redes ethernet basada en puertos de red. Fue originalmente creada para exigir a los usuarios autenticarse antes de obtener los privilegios de red; sin embargo, esta fue adaptada para ser utilizada en este tipo de ambiente. El wireless EAP ha sido mejorado para incluir la encriptación en la capa de transporte y administración de llaves.

   Esta nueva característica es importante, ya que elimina el riesgo de la administración estática de las llaves por parte de WEP.EAP utiliza un servidor RADIUS para administrar de manera centralizada las credenciales y los registros de usuarios (Accounting). Esta administración centralizada elimina la necesidad de los administradores para realizar actualizaciones manuales de las llaves estáticas, como en el protocolo WEP y de las direcciones MAC de numerosos AP algunos de los tipos de EAP son los siguientes:

   - ✓ EAP-MD5: Provee un robusto mecanismo de autenticación utilizando el algoritmo hash MD5, en vez de un password en texto plano.
   - ✓ EAP-TLS: Provee la administración de las llaves para la encriptación de la capa de transporte.
   - ✓ EAP-TTLS: Es similar al modelo EAP-TLS, pero utiliza servidores certificados (Server Certificates).

   Algunos de los beneficios de este modelo son los siguientes:

- ✓ Reducción o eliminación de las vulnerabilidades de WEP.
- ✓ Administración centralizada de las direcciones MAC y de los usuarios.
- ✓ Reportes de actividades (Accounting) acerca de las actividades de acceso y autorización.
- ✓ Interoperatividad: RADIUS es soportado por una gran cantidad de fabricantes de AP y clientes Wireless.

6. **IPSEC (Internet Protocol security).** Es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y, de esta manera, asegurar las comunicaciones a través de dicho protocolo. Inicialmente fue desarrollado para usarse con el nuevo estándar IPv6 aunque posteriormente se adaptó a IPv4. Presenta un gran nivel de seguridad y compatibilidad, también denominado Wireless VPN. Debido a la gran popularidad en redes alambradas, IPSEC es normalmente recomendado como una solución para resolver las implementaciones de seguridad que presentan anomalías en redes Wireless. Muchas organizaciones utilizan IPSEC debido a que cuentan con la infraestructura adecuada y disponible para implementar un cliente remoto utilizando VPN, puesto que los costos y las horas hombre utilizadas son mínimos. Los beneficios de la aplicación de IPSEC en redes WiFi son los siguientes:

- ✓ Provee un alto nivel de seguridad: IPSEC se usa en funcionalidades que chequean la integridad, autenticación mutua y anti-replay.
- ✓ Permite interoperatividad: A diferencia de otros sistemas, hoy en día IPSEC es un estándar maduro y de alto grado de utilización.

- ✓ Repara los errores del diseño de redes de WiFi. VPN Wireless es la mejor opción para remediar la seguridad en redes WLAN, ya sea por un mal diseño o porque los estándares de diseños no son los adecuados, esta opción permite eliminar cualquier problema de seguridad sin tener que realizar inversiones por dispositivos adicionales.
- ✓ Existe una nueva forma de establecer túneles mediante los llamados "Clientless" VPN, los cuales no requieren implementar IPSEC en los clientes, sino que existe un sólo mecanismo centralizado que realiza esta función, dejando la tarea de encriptación por parte del cliente a aplicaciones de capa superiores.

7. **AES (Advanced Encription Standard).** Es un robusto esquema de encripción adoptado como estándar de seguridad por algunos estamentos gubernamentales en E.U y por NIST (National Institute of Standards and Technology), que junto al 802.1x/EAP (Extensible Authentication Protocol) y Preshared Key, encripción y autenticación hacen para WPA2 la versión completa del estándar de seguridad en redes inalámbricas (IEEE 802.11i.802.1x/EAP) utiliza Servidor Radius (Remote Authentication Dial In User Service) en la red cableada para autenticar usuarios. Requiere Cliente 802.1x en la estación de trabajo. Preshared Key, utiliza una llave secreta. No requiere Servidor Radius. También es llamada "WPA Personal".

ESTÁNDARES PARA REDES INALÁMBRICAS

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras –Seguras– Temporales), y AES (Estándar de Encriptación Avanzado).

COMPARACIÓN TECNOLOGÍAS INALÁMBRICAS MÓVILES

Tipo de red	WWAN (Wireless WAN)	WLAN (Wireless LAN)	WPAN (Wireless Personal Area Network)
Estándar	GSM/GPRS/UMTS	IEEE 802.11 (WiFi)	IEEE 802.15 (Bluetooth)
Velocidad	9,6/170/2000 Kb/s	1-2-11-54 Mb/s(*)	721 Kb/s
Frecuencia	0,9/1,8/2,1 GHz	2,4 y 5 GHz Infrarrojos	2,4 GHz
Rango	35 Km	70 - 150 m	10 m
Técnica radio	Varias	FHSS, DSSS, OFDM	FHSS
Itinerancia (roaming)	Sí	Sí	No
Equivalente a:	Conexión telef. (módem)	LAN	Cables de conexión

Conclusiones

Como hemos descrito en los apartes anteriores, las redes inalámbricas serán de fácil violabilidad y penetración si los administradores no tienen y adecuan políticas de seguridad. La mejor defensa es tener prevista una serie de reglas que permitan el acceso a intrusos. Para ello, convendría seguir estos consejos, que nos permitirían controlar en un gran porcentaje nuestra red.

- ✓ Cambiar las claves por defecto cuando instalemos el software del Punto de Acceso.
- ✓ Control de acceso seguro con autenticación bidireccional.
- ✓ Control y filtrado de direcciones MAC e identificadores de red para restringir los adaptadores y puntos de acceso que se puedan conectar a la red.
- ✓ Configuración WEP; la seguridad del cifrado de paquetes que se transmiten es fundamental. La codificación puede ser más o menos segura, dependiendo del tamaño de la clave creada y su nivel; la mas recomendable es de 128 Bits.
- ✓ Crear varias claves WEP, para el punto de acceso y los clientes y que varíen cada día.

✓ Utilizar opciones no compatibles; si nuestra red es de una misma marca, podemos escoger esta opción para tener un punto más de seguridad; esto hará que nuestro posible intruso tenga que trabajar con un modelo compatible al nuestro.

Bibliografía

Carlos Aracena Urrutia, Cristian Araya Valenzuela. Seguridad en redes WiFi Entel S.A / Americatel Corp. p://www.senacitel.cl/downloads/senacitel2004/tt42.pdf.

Curso Seguridad en WiFi y redes WiMax. http://netacad.uv.es/campus-ti.htm.

Laura Gonzalo.Soluciones R/S para banda Ancha. laura.gonzalo@rohde.schwarz.com.

Glosario de Seguridad Informática. http://www.virusprot.com/Glosarioc.html.

Fourouzam Behrouz A. Transmisión de Datos y Redes de comunicaciones.

Manual- Curso de Certificación DPC. D'Link Partner Certification D-Suppor for Wireless. Cartagena Colombia.

Conceptos de seguridad en redes inalámbricas 802.11. http://www.gui.uva.es.