ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
Facultad de Ingeniera en Electricidad y Computación

Tema:

Seguridad en Redes Inalámbricas.

Integrantes:

Geannina Jackeline Aguirre Briones [1]

Angela Isabel Sanclemente Ordóñez[2]

Laura Alexandra Ureta Arreaga[3]

Ing. Albert Espinal Santana[4]

[1]Licenciado en Sistemas de Información 2005; email: geagus1@yahoo.es

[2]Licenciado en Sistemas de Información 2005; email: angiesanclemente17@hotmail.com

[3]Licenciado en Sistemas de Información 2005; email: alexa_ua2002@yahoo.com.mx

[4]Director de Tópico, Título de Pregrado: Ingeniero en Computación, ESPOL, Diciembre 1996. Título de Postgrado: Magister en Sistemas de Información Gerencial, ESPOL, Enero 2000. Profesor de la ESPOL desde: Octubre 1996

RESUMEN

El constante avance tecnológico nos exige mejorar ciertas actividades e implementar nuevas tecnologías, como es la implementación de las redes inalambricas. Por ésta razón, nosotras hemos realizado un profundo estudio sobre los niveles de seguridad que se deben considerar en la implementación de las redes inalámbricas, los cual le permitirá a una empresar garantizar la seguridad de la información que por ella transita.

Nuestro objetivo es dar a conocer los diferentes tipos de ataques informáticos a los cuales están expuestas las redes inalámbricas, así como también presentar los niveles y metodogías de seguridad que se deben considerar cuando se implementa una solución de este tipo.

En la primera parte de este documento se especifican la conceptualización de redes inalambrica así como sus vulnerabilidades o tipos de ataque a lo que están expuestas. Posteriormente se detallan las metodologías de seguridad disponibles y el análisis de cada una de ellas.

SUMMARY

The constant technological advance force us to improve certain activities and to implement new technologies like the implementation of the wireless net . For these reason we have realized a profound study about the level of security that must be considered in the implementation of the wireless net That which will permit a company to guarantee the security of the information that traffics for her.

Our goals is to give to know the different types of information attacks that which the wireless net is expose to, as well as to present the levels and methodologies of security that must be considered when a solution of this type is implemented.

In the first part of this document is specific the conceptualization of wireless net, as well as their vulnerabilities or types of attacks that they are expose. Later on the available methodologies of security are detailed, and the analysis of each one of them .

INTRODUCCIÓN

Las redes inalámbricas de área local (WLAN) tienen un papel cada vez más importante en las comunicaciones del mundo de hoy. Debido a su facilidad de instalación y conexión, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta inconveniente o imposible brindar servicio con una red alambrada. La popularidad de estas redes ha crecido a tal punto que los fabricantes de computadores y motherboards están integrando dispositivos para acceso a WLAN en sus equipos.

Por lo tanto, hemos podido desarrollar el tema de "Seguridades en redes Inalámbricas", presentando y exponiendo las diferentes inquietudes y necesidades de cada uno de nuestras fuentes de información(personas, empresas , etc).

A continuación, se da a conocer el presente trabajo esperando que en el, se encuentre una guía en cuanto a los niveles básicos y avanzados de seguridad que se deben considerar en la implementación de redes inalámbricas.

CONTENIDO

1. Generalidades.

Una red de área local inalámbrica puede definirse, como a una red de alcance local que tiene como medio de transmisión el aire; también llamada Wireless Lan (WLAN), es un sistema flexible de comunicaciones que puede implementarse como una extensión o directamente como una alternativa a una red cableada.

Las ventajas de las WLAN con relación a las redes LAN cableadas son su Movilidad, Facilidad y rapidez en la instalación, Flexibilidad, Reducción de costos, y Escalabilidad.

2. Vulnerabilidades en Redes Wireless LAN.

¿Porqué las redes inalámbricas sean más vulnerables que las redes de cable? .

La respuesta es sencilla: desconocimiento de las herramientas de seguridad disponibles para redes inalámbricas.

2.1 Principales Debilidades.

2.1.1 Ataques de escucha/monitorización pasiva (eavesdropping).

La autenticación es posible tras la captura y *cracking* de cierto número de paquetes. Es posible accesar y monitorizar del tráfico presente en el entorno como cualquier cliente autenticado. También es posible realizar inyección y modificación de mensajes, sin necesidad de descifrar claves.

2.1.2. Ataques de Intercepción/Inserción (man-in- the-middle).

Los entornos que operan sobre el protocolo 802.11b facilitan la captura y redirección de sesiones, ya que una estación que transmite no es capaz de detectar la presencia de estaciones adyacentes con la misma dirección MAC o IP. Esto permite que se lleve a cabo un ataque de secuestro de sesión mediante el uso de dos estaciones hostiles diferentes.

2.1.3. Ataques de denegación de servicio (jam-ming).

Es sencillo realizar ataques que afecten a la disponibilidad en los entornos *wireless.* Dichos ataques pueden ser abordados desde varios enfoques, siendo los más sencillos aquellos que utilizan un dispositivo de radiofrecuencia (RF) de alta potencia para generar interferencias, lo que prevendría que el usuario legitimo pudiera utilizar el servicio.

2.1.4. Interferencia y Atenuación

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por materiales medioambientales.

Material	Ejemplo	Interferencia
Madera	Tabiques	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Arboles y plantas	Media
Agua	Lluvia	Alta
Cerámica	Tejas	Alta
Metal	Vigas, armarios	Muy Alta

Tabla 1 Interferencia y Atenuación

2.2. El Problema De La Seguridad

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica.

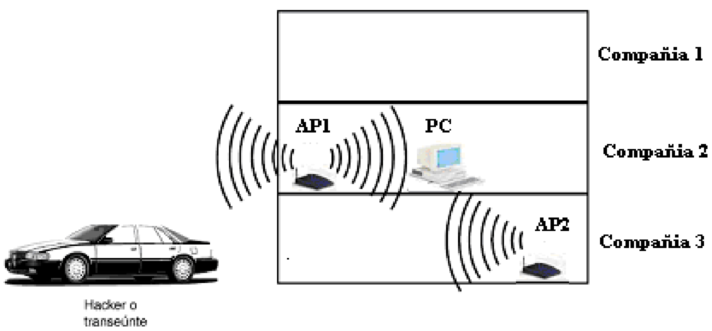

Fig. 1 Acceso no autorizado a una red inalámbrica.

2.3. Localizando Redes Inalámbricas

2.3.1. Warchalking

Consiste en caminar por la calle con un computador portátil dotado de una tarjeta WLAN, buscando la señal de puntos de acceso. Cuando se encuentra uno, se pinta con tiza un símbolo especial en la acera o en un muro, indicando su presencia y nivel de seguridas.

2.3.2. Wardriving

Consiste en localizar puntos de acceso inalámbrico desde un automóvil. Para este fin se necesita un computador portátil con tarjeta WLAN, una antena adecuada, un GPS para localizar los puntos de acceso, y software para detección de redes inalámbricas.

3. Seguridad Básica y Avanzada en Wireless LAN

Existen métodos para lograr la configuración segura de una red inalámbrica;

3.1. Método 1: Filtrado de direcciones MAC

Este método consiste en 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.

3.2. Método 2: Wired Equivalent Privacy (WEP)

El nivel más básico de seguridad para redes inalámbricas es el algoritmo WEP, ha sido diseñado para prevenir posibles escuchas de la información y proteger la red mediante la encriptación de los datos que se envíen de forma inalámbrica. Existen situaciones que hacen que WEP no sea seguro:

- La mayoría de instalaciones emplea WEP con claves de cifrado estáticas.
- WEP sólo cubre el segmento *wireless* de la comunicación.
- El IV que se utiliza es de longitud insuficiente (24 bits).

- Wep no ofrece servicio de autenticación.

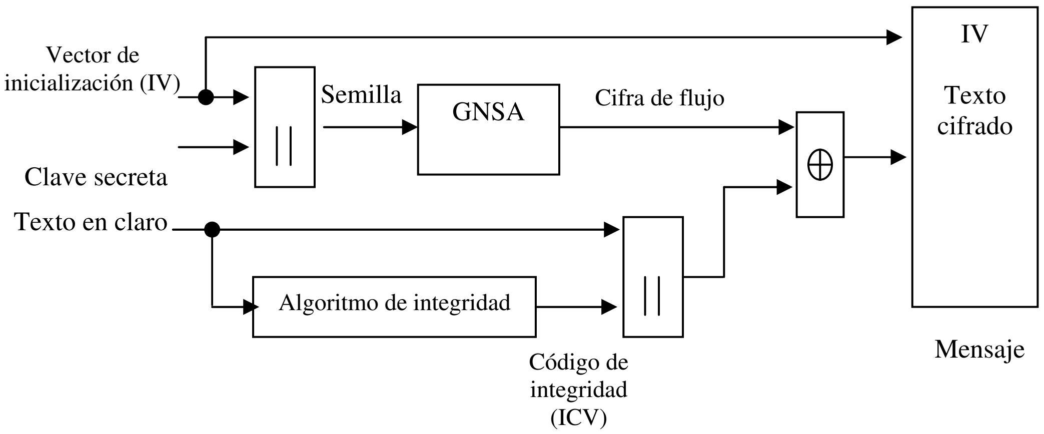

Fig. 2 Funcionamiento del algoritmo WEP en modalidad de cifrado.

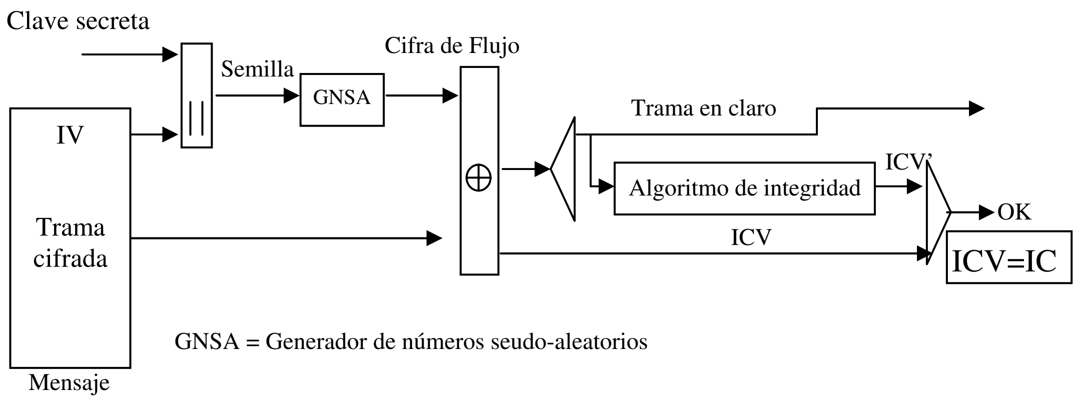

Fig. 3 Funcionamiento del algoritmo WEP en modalidad de descifrado.

3.3. Método 3: Las 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.

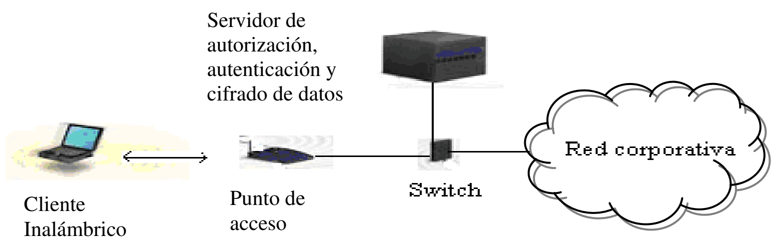

Fig. 4 Estructura de una VPN para acceso inalámbrico seguro.

3.4. Método 4: 802.1x

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas.

Fig. 5 Arquitectura de un sistema de autenticación 802.1x.

3.5. Método 5: Wpa (Wi-Fi Protected Access)

WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. TKIP amplía la longitud de la clave de 40 a 128 bits.

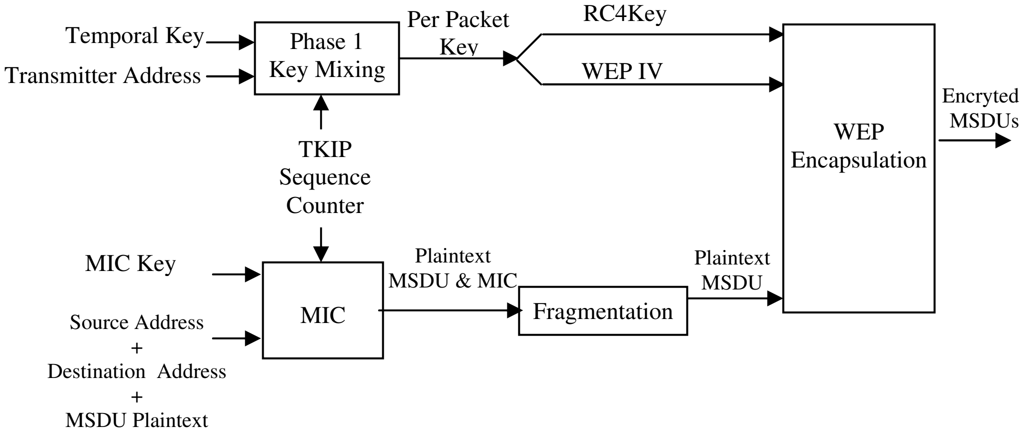

Fig. 6 Proceso de Encapsulación TKIP

CONCLUSIONES

La seguridad en las redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite. Sin embargo, muchas redes inalámbricas instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, lo que pone en peligro la confidencialidad e integridad de dicha información.

La implementación de la seguridad depende del uso que se vaya a dar a la red (casera o empresarial), si es una red existente o nueva, y del presupuesto del que se disponga para implantarla.

La restricción de acceso mediante direcciones MAC es insuficiente, dado el gran número de herramientas disponibles libremente para cambiar la dirección MAC de una tarjeta.

El método mediante WEP con clave estática es el mínimo nivel de protección que existe. En una red casera puede ser suficiente; en una corporativa, su uso está desaconsejado, por la facilidad con la que se pueden romper las claves WEP en un entorno de alto tráfico.

VPN es una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x. Requiere de la instalación de software especializado en los clientes inalámbricos, y de uno o más servidores que manejen las tareas de cifrado de datos, autenticación y autorización de acceso.

La alternativa de 802.1x y EAP es la adecuada si los equipos de la red inalámbrica se pueden actualizar, o si se va a montar una red nueva.

Finalmente, todo mecanismo de protección de información en una red debe estar enmarcado dentro de una política de seguridad adecuada.

REFERENCIAS

a) Tesis

1. I. García, M. Montalvo, X. Zavala, "Gestion de una red Lan Inalámbrica usando herramienta propietaria basada en SNMP", (Tesis, Ingeniería Electrónica, Facultad de Ingeniería Electrica y Computación, Escuela Superior Politécnica del Litoral, 2002).

c) Documentación sobre conceptos, tecnologías, normativas y seguridades en redes inalámbricas

1. http:// www.sgi.es/prensa/articulos_interes/sic52-art_javier_megias.PDF, pp 1-2

2. http:// www.maestrosdelweb.com/editorial/redeswlan/, pp 3-4

4. http:// www.icesi.edu.co, pp 3-9

5. http:// http://www.hispasec.com/unaaldia/1486, pp 3-6

6. http:// http://www.saulo.net, pp 3-10

Ing. Albert Espinal Santana,

Director de Tesis