CAPITULO 3

DESCRIPCION DE PROTECCIONES EN REDES INALÁMBRICAS.

En la actualidad uno busca conectarse a una red que nos pueda brindar de cierta manera un tipo de protección, las cuales no son tan conocidas dado que están entrando apenas al país y el proveedor del dispositivo o de la conexión inalámbrica no brinda una explicación breve de las protecciones que brinda el producto inalámbrico, con o cual podríamos perder protección en seguridad, por lo cual explicaremos brevemente algunas de ellas.

3.1 Red Privada Virtual (VPN)

Una VPN es una red privada, fue construida sobre la infraestructura de una red pública (recurso público, sin control sobre el acceso de los datos), normalmente Internet. Es decir, en vez de utilizarse enlaces dedicados (como el X.25 y *Frame Relay*) para conectar redes remotas, se utiliza la infraestructura de Internet, una vez que las redes están conectadas es transparente para los usuarios.

La principal motivación para la implantación de las VPN es la financiera: los enlaces dedicados son demasiados caros, principalmente cuando las distancias son largas. Por otro lado existe Internet, que por ser una red de alcance mundial, tiene puntos de presencia diseminados por el mundo. Las conexiones con Internet tienen un costo mas bajo que los enlaces dedicados, principalmente cuando las distancias son largas.

Internet es una red pública, donde los datos en transito pueden ser "leídos por cualquier equipo". La seguridad en la comunicación entre las redes privadas es imprescindible, se hace necesaria una forma de cambiar los datos codificados, de forma que si fuesen capturados durante la transmisión, no puedan ser descifrados. Los datos transitan codificados por Internet en "Túneles Virtuales" creados por dispositivos VPN que utilizan criptografía y esos dispositivos que son capaces de "entender" los datos codificados forman, una "red virtual" sobre la red pública. Es esa red virtual la que es conocida como VPN. [WAGU]

Los dispositivos responsables para la formación y administración de la red virtual, para propiciar una comunicación con seguridad, deben ser capaces de garantizar:

La seguridad de los datos, en el caso que fuesen interceptados durante la transmisión, no pueden ser decodificados.

Integridad de los datos, además de no ser descodificados (seguridad), los datos no pueden ser modificados durante la transmisión.

La autenticación, es garantía de que los datos están siendo trasmitidos o recibidos del dispositivo remoto autorizado y no de un equipo cualquiera, es decir, es garantía de que el dispositivo remoto con el cual fue establecido el túnel es el dispositivo remoto autorizado y no otro equipamiento haciendolo pasar por él. [ITCUR]

3.2 MAC Address.

Todos los ordenadores de una misma red comparten el mismo medio, por lo que debe de existir un identificador único para cada equipo, o mejor dicho para cada tarjeta de red. Esto no sucede en una conexión telefónica mediante modem, ya que se supone que cualquier dato que se envía está destinado al equipo que se encuentra al otro lado de la línea. Pero cuando se envían datos en una red local, hay que especificar claramente a quien van dirigidos. Esto se consigue mediante la dirección MAC, un número compuesto por 12 dígitos hexadecimales que identifica de forma única a cada dispositivo ethernet. La dirección MAC se compone de 48 bits. Los 24 primeros bits identifican al fabricante del hardware, y los 24 bits restantes corresponden al número de serie asignado por el fabricante, lo que garantiza que dos tarjetas no puedan tener la misma dirección MAC. Direcciones MAC duplicadas causarían problemas en la red. [HACK03]

3.2.1 Filtrado de direcciones MAC (Médium Acces Control):

Este método consiste en que se crea una base de datos en cada uno de los puntos de acceso de las direcciones MAC de cada tarjeta inalámbrica que cuenten con autorización para poder acceder a la red. Como cada tarjeta posee una dirección única MAC se logra autentificar el equipo. [HACK03]

3.3 WEP (*Wired Equivalent Protocol*)

Es un sistema de encriptación estándar propuesto por el comité 802.11, implementado a nivel de la capa MAC del modelo OSI. Dicho estándar comprime y cifra los datos que se envían a través de las ondas de radio. [MEDEIE]

Con la protección WEP, la tarjeta de red encripta el cuerpo y el CRC de cada trama 802.11 antes de la transmisión utilizando el algoritmo de encriptación RC4, proporcionado por RC4[1]Security. La estación receptora, sea un punto de n receptora, sea un punto de acceso o una estación cliente, es quien se encarga de desencriptar los datos. Este método forma parte de la especificación 802.11 y esta diseñado para proteger la transmisión mediante un cifrado, la WEP trabaja en el nivel 2 del modelo OSI (enlace de datos), es uno de los métodos más complejos, aunque existen programas para romper dicha protección.
En la figura 13 podemos observar la manera en que se hace la encriptación de la protección WEP [HACK03], los pasos a seguir son:

Paso 1 demuestra que el RC4 utiliza la combinación de la llave compartida y IV para producir una llave dominante para cada paquete.

Paso 2 demuestra que la longitud de la llave dominante es igual a la longitud del paquete, puesto que los bits de datos en el paquete tienen que hacer un XOR con la llave dominante para generar el texto del texto cifrado.

[1] RC4 es un cifrador diseñada por Rivest para la seguridad de datos de RSA (ahora seguridad de RSA)

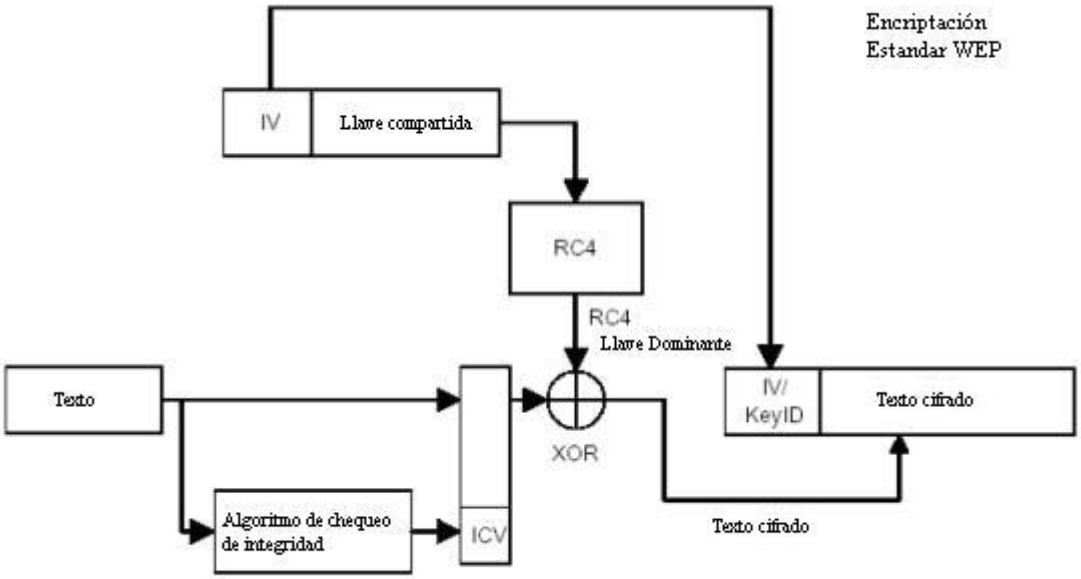

Figura 13. Diagrama del WEP [INSEG]

Usar una llave separada para cada paquete soluciona el problema de la sincronización pero realiza uno de los requisitos más importantes de RC4 es que la misma llave no se debe reutilizar siempre. Este requisito, combinado con el hecho 802.11 necesitaría una nueva llave para cada paquete haría la red realmente segura, significa que 802.11 necesitaría un espacio dominante muy grande. Puesto que 802.11 no especifica ninguna manera de compartir una llave, la mayoría 802.11 pone en práctica la utilización de la misma llave en un BSS. El fondo es ése para todos los propósitos prácticos que la llave que es utilizada por RC4 es una concatenación de una constante (la llave precompartida) y del IV. Por lo tanto, el espacio dominante para el RC4 es 2N donde está la longitud N del IV. 802.11 especifica la longitud del IV como 24. [HACK03]

3.4 Protección 802.1x

Es un mecanismo estándar para autenticar centralmente estaciones y usuarios, es un estándar abierto que soporta diferentes algoritmos de encriptación. Se apoya en el protocolo de autenticación EAP (*Extensible Authentication Protocol*), aunque en realidad es EAPoL (*Extensible Authentication Protocol over LAN*) de forma que se puede usar en redes alámbricas, 802.11, Token-Ring y FDDI (*Fiber Distributed Data Interface*). Requiere cliente, Punto de Acceso y servidor de autenticación. EAP es soportado por muchos Puntos de Acceso y por HostAP. Antes de la autenticación sólo se permite tráfico 802.1X (petición de autenticación). [HACK03]

3.5 WPA (*Wi-Fi Protected Access*).

Es un estándar que se ha propuesto por los miembros de la *Wi-Fi Alliance* en colaboración con la IEEE, el cual busca subsanar los problemas de WEP, mejorando el cifrado y un mecanismo de autenticación, el cual emplea el 802.1x y EAP (Extensible Authentication Protocol). Resuelve los inconvenientes de la encriptación de la Privacidad Equivalente Cableada (WEP), utilizando el Protocolo de Integridad de Llave temporal (TKIP), el cual se envuelve alrededor de la WEP y cierra sus hoyos de seguridad. El Acceso Protegido Wi-Fi (WPA), incluye además los beneficios de autenticación del estándar 802.1X. [HACK03]