Capítulo 4

Protocolos y técnicas alternativas al WEP.

En este capítulo se presentan algunos protocolos y técnicas que ofrecen mayores garantías en seguridad en redes inalámbricas, eliminando las debilidades características del WEP.

4.1 Estándar IEEE 802.1X.

Este estándar define tres entidades, el usuario solicitante que busca el puerto control de acceso, el servidor de autenticación que concede o niega la autenticación y el autenticador, el cual lleva a cabo el intercambio de autenticación entre el solicitante y el servidor de autenticación. El servidor autenticador tiene información única de cada cliente autorizado y para concederle acceso, el servidor compara las credenciales proporcionadas por el solicitante con la información en su base de datos [BOR05].

4.2 Red privada virtual (VPN).

El uso tanto de redes públicas como privadas para crear una conexión de red se denomina red privada virtual (VPN). Una red privada virtual es la extensión de una red privada que comprende vínculos en redes compartidas o públicas como Internet. Con una VPN se pueden transmitir datos entre dos equipos a través de una red compartida o pública imitando el funcionamiento de un vínculo privado punto a punto.

Para imitar un vínculo punto a punto, los datos se encapsulan o se envuelven con un encabezado que proporciona información de enrutamiento, lo que permite que los datos atraviesen la red compartida o pública hasta llegar a su punto de destino. Para imitar un vínculo privado, los datos se cifran para conservar la confidencialidad. Los paquetes interceptados en la red compartida o pública no se pueden descifrar sin las claves de cifrado. El vínculo en el que se encapsulan y se cifran los datos privados es una conexión de red privada virtual [VPN06]. La Figura 4.1 muestra el diagrama de una posible red privada virtual conectando a una red LAN y WLAN a Internet a través de un servidor VPN.

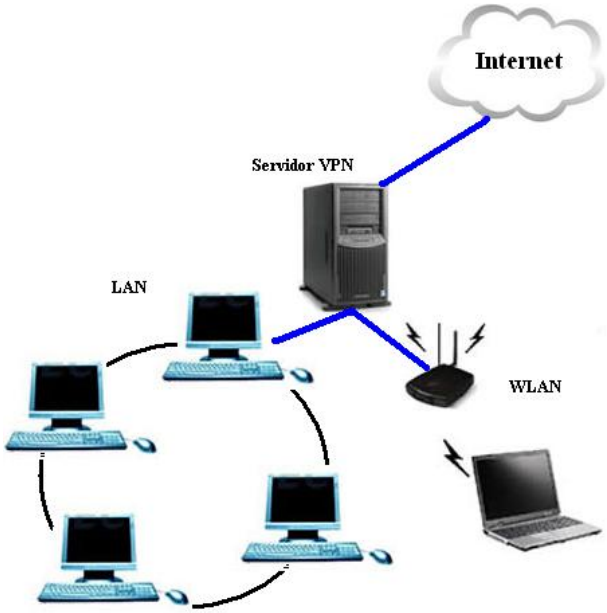

Figura 4.1 Red privada virtual.

4.3 Capa de sockets seguros (SSL).

El cifrado de capa de sockets seguros (SSL, *Secure Sockets Layer*) es el método más utilizado para transmitir datos cifrados por Internet. Este funciona mediante el

intercambio de llaves entre el cliente y el servidor que sirven para descifrar la información que ha sido codificada por un cifrado simétrico. De esta forma los datos encriptados pueden ser decriptados únicamente por el poseedor de la llave correcta [BOR05].

La Figura 4.2 ilustra los pasos que se realizan para establecer una sesión SSL.

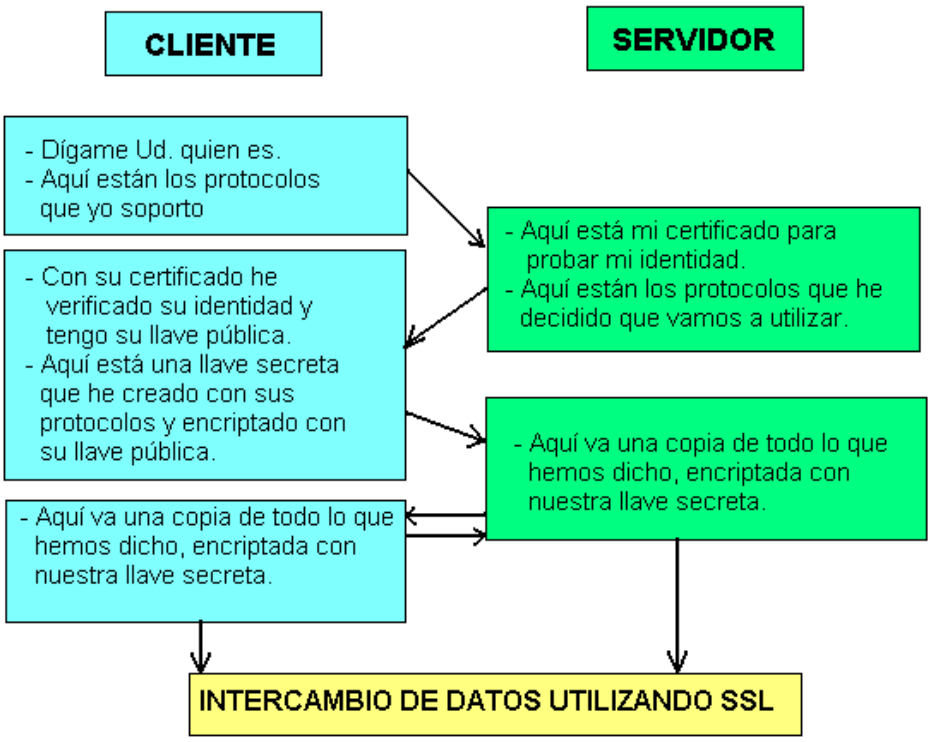

Figura 4.2 Pasos pasa establecer una sesión SSL [SSL06]

Finalmente, cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión SSL [SSL06].

4.4 Temporal Key Integrity Protocol (TKIP).

Tiene cuatro componentes: mensaje criptográfico (MIC), secuenciado de paquetes, llaves por paquete y mecanismo de “re-llaveo”.

i) MIC: Un generador pseudoaleatorio o *hash* usa una llave de integridad para calcular el MIC de la dirección MAC fuente, destino y cuerpo de frame. El MIC se incluye en el contador encriptado de la trama. El receptor aplica la función *hash* al mensaje recibido usando su llave de integridad. Si el cálculo del receptor muestra una concordancia entre el MIC enviado y el mensaje, entonces se presume auténtico.

ii) Secuenciado de paquetes: TKIP asocia un número de secuencia con la encriptación TKIP. Una parte del paquete WEP IV se reutiliza por el número de secuencia TKIP, el cual es de 16 bits. Por cada nueva llave de encriptación TKIP, el número de secuencia se inicializa con ‘0’ y se incrementa con cada paquete.

iii) Llaves por paquete: TKIP usa una llave temporal y el número de secuencia del paquete. La llave temporal es secreta y compartida entre transmisor y receptor, es de 128 bits.

iiii) “Re-llaveo”: TKIP usa tres llaves temporales, la llave de encriptación y las llaves maestras. La llave maestra se usa para comunicar un conjunto de llaves de encriptación entre el cliente y un punto de acceso. Las llaves de encriptación se usan para asegurar los mensajes que contienen material que el cliente y el punto de acceso necesitan para calcular un par de llaves temporales [BOR05].

4.5 Acceso protegido de fidelidad inalámbrica (WPA).

La *Wi-Fi Alliance*, trabajando en conjunto con el IEEE, desarrolló esta especificación de seguridad para eliminar las vulnerabilidades del WEP. WPA se desarrolló para ser utilizado con cualquier equipo a través de actualizaciones del *firmware*.

WPA incrementa de forma importante el nivel de protección para datos que circulan por el aire en redes Wi-Fi actuales y futuras. WPA elimina todas las debilidades del WEP. Aunque no es una solución segura "a prueba de balas", WPA representa un paso importante en la seguridad de redes inalámbricas. WPA está diseñado para ser compatible con dispositivos 802.11, incluyendo los estándares 802.11b, 802.11a y 802.11g, y forma parte del estándar 802.11i, en el cual se conoce como WPA2. Cuando se instala correctamente, provee a los usuarios de redes WLAN con in nivel alto para asegurar que sus datos permanezcan protegidos y que sólo usuarios autorizados puedan acceder a sus redes.

El algoritmo de encriptación, TKIP, utilizado en WPA es, al igual que el WEP, basado en el algoritmo RC4, aunque con modificaciones importantes. La longitud del vector de inicialización se incrementó a 48 bits y las llaves compartidas se cambian en cada sesión. Esto significa que la interceptación de tráfico protegido por WPA no es una tarea fácil y no se conocen ataques teóricos o prácticos contra dicho protocolo. El proceso de autenticación se realiza con el protocolo 802.1X [WIF03].

4.6 Estándar 802.11i y WPA2 (Acceso protegido de fidelidad inalámbrica 2)

WPA2 está basado en el estándar IEEE 802.11i. WPA2 es la implementación aprobada por *Wi-Fi Alliance* del estándar 802.11i y es compatible con WPA. WPA2 provee un alto nivel de seguridad incluyendo el algoritmo AES (Sistema Avanzado de Encriptación). WPA2 puede habilitarse en dos versiones: WPA2 *Personal* y WPA2 *Enterprise*. WPA2 *Personal* protege de acceso no autorizado a la red utilizando una contraseña establecida. WPA2 *Enterprise* verifica a los usuarios de la red a través de un servidor [WPA06].

El AES utiliza una llave temporal de 128 bits y un vector de inicialización de de 48 bits en el proceso de encriptación. Los métodos de autenticación utilizados por el 802.11i utilizan el estándar IEEE 802.11X y el protocolo TKIP [BOR05].

4.7 Técnica de Inserción de Caracteres Falsos y Compresión (FCICT, *Fake Character Insertions and Compression Technique*)

Esta técnica implementa una mejora en el WEP, al actuar directamente en el cifrado generado por el algoritmo RC4. La técnica FCICT [CHA05] inserta caracteres falsos en el texto cifrado y lo envía al receptor. El receptor identifica los caracteres falsos y los elimina para poder decriptar los datos usando el RC4. Un intruso que intercepte el texto cifrado, tendría que determinar los caracteres falsos primeramente, antes de decriptar la información. Este proceso elimina algunas debilidades del WEP y se explica detalladamente en el capítulo 5.