SEGURIDAD EN REDES INALÁMBRICAS

TRABAJO AMPLIACIÓN DE REDES
5º INGENIERÍA INFORMÁTICA
UNIVERSITAT DE VALÈNCIA

Alumno: Vicent Alapont Miquel

Índice de tablas y figuras

1. INTRODUCCIÓN

La irrupción de la nueva tecnología de comunicación basada en redes inalámbricas ha proporcionado nuevas expectativas de futuros para el desarrollo de sistemas de comunicación, así como nuevos riesgos.

La flexibilidad y la movilidad que nos proporcionan las nuevas redes inalámbricas han hecho que la utilización de estas redes se hayan disparado en el año 2002 siendo la mejor manera de realizar conectividad de datos en edificios sin necesidad de cablearlos.

Pero como todas la nuevas tecnologías en evolución, presenta unos riesgos debidos al optimismo inicial y en la adopción de la nueva tecnología sin observar los riesgos inherentes a la utilización de un medio de transmisión tan 'observable' como son las ondas de radio.

El presente trabajo pretende dar una visión global del estado actual de la seguridad en las redes inalámbricas, desde los riesgos existentes en las implementaciones de los estándares actuales, hasta las mejoras propuestas para subsanar dichos riesgos pasando por consideraciones recomendadas en cuando al diseño de redes inalámbricas.

Por último, quería denotar que mientras me encontraba redactando la presente memoria, han aparecido nuevas vulnerabilidades de diversos protocolos que más tarde serán explicados. Por lo tanto, con el deseo de que esta memoria no quede obsoleta antes de salir publicada, espero que los apartados tratados sean de interés para el lector.

2. RIESGOS DE LAS REDES INALAMBRICAS

Aunque este trabajo vaya dirigido a los aspectos de seguridad de la red inalámbrica, no podemos pasar por alto los elementos que componen la red inalámbrica.

Existen 4 tipos de redes inalámbricas, la basada en tecnología BlueTooth, la IrDa (Infrared Data Association), la HomeRF y la WECA (Wi-Fi). La primera de ellas no permite la transmisión de grandes cantidades de datos entre ordenadores de forma continua y la segunda tecnología, estándar utilizado por los dispositivos de ondas infrarrojas, debe permitir la visión directa entre los dos elementos comunicantes. Las tecnología HomeRF y Wi-Fi están basados en las especificaciones 802.11 (Ethernet Inalámbrica) y son las que utilizan actualmente las tarjetas de red inalámbricas.

La topología de estas redes consta de dos elementos clave, las estaciones cliente (STA) y los puntos de acceso (AP). La comunicación puede realizarse directamente entre estaciones cliente o a través del AP. El intercambio de datos sólo es posible cuando existe una autentificación entre el STA y el AP y se produce la asociación entre ellos (un STA pertenece a un AP). Por defecto, el AP transmite señales de gestión

periódicas, el STA las recibe e inicia la autentificación mediante el envío de una trama de autentificación. Una vez realizada esta, la estación cliente envía una trama asociada y el AP responde con otra.

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad. La salida de estas ondas de radio fuera del edificio donde está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible a la empresa y a la seguridad informática de la misma.

Varios son los riesgos derivables de este factor. Por ejemplo, se podría perpetrar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal más potente que capte las estaciones cliente en vez del punto de acceso legítimo, interceptando la red inalámbrica. También seria posible crear interferencias y una más que posible denegación de servicio con solo introducir un dispositivo que emita ondas de radio a una frecuencia de 2'4GHz (frecuencia utilizada por las redes inalámbricas).

La posibilidad de comunicarnos entre estaciones cliente directamente, sin pasar por el punto de acceso permitiría atacar directamente a una estación cliente, generando problemas si esta estación cliente ofrece servicios TCP/IP o comparte ficheros. Existe también la posibilidad de duplicar las direcciones IP o MAC de estaciones cliente legítimas.

Los puntos de acceso están expuestos a un ataque de Fuerza bruta para averiguar los passwords, por lo que una configuración incorrecta de los mismos facilitaría la irrupción en una red inalámbrica por parte de intrusos.

A pesar de los riesgos anteriormente expuestos, existen soluciones y mecanismos de seguridad para impedir que cualquiera con los materiales suficientes pueda introducirse en una red. Unos mecanismos son seguros, otros, como el protocolo WEP fácilmente 'rompibles' por programas distribuidos gratuitamente por Internet.

3. MECANISMOS DE SEGURIDAD

3.1 WEP (Wired Equivalent Protocol)

El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de vendedores de soluciones inalámbricas. En ningún caso es comparable con IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio.

Con 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 RSA Security. La estación receptora, sea un punto de acceso o una estación cliente es la encargada de desencriptar la trama.

Como parte del proceso de encriptación, WEP prepara una estructura denominada ‘seed’ obtenida tras la concatenación de la llave secreta proporcionada por el usuario de la estación emisora con un vector de inicialización (IV) de 24 bits generada aleatoriamente. La estación cambia el IV para cada trama transmitida.

A continuación, WEP utiliza el ‘seed’ en un generador de números pseudo-aleatorio que produce una llave de longitud igual a el payload (cuerpo más CRC) de la trama más un valor para chequear la integridad (ICV) de 32 bits de longitud.

El ICV es un checksum que utiliza la estación receptora para recalcularla y compararla con la enviada por la estación emisora para determinar si los datos han sido manipulados durante su envío. Si la estación receptora recalcula un ICV que no concuerda con el recibido en la trama, esta queda descartada e incluso puede rechazar al emisor de la misma.

WEP especifica una llave secreta compartida de 40 o 64 bits para encriptar y desencriptar, utilizando la encriptación simétrica.

Antes de que tome lugar la transmisión, WEP combina la llave con el payload/ICV a través de un proceso XOR a nivel de bit que producirá el texto cifrado. Incluyendo el IV sin encriptar sin los primeros bytes del cuerpo de la trama.

La estación receptora utiliza el IV proporcionado junto con la llave del usuario de la estación receptora para desencriptar la parte del payload del cuerpo de la trama.

Cuando se transmiten mensajes con el mismo encabezado, por ejemplo el FROM de un correo, el principio de cada payload encriptado será el mismo si se utiliza la misma llave. Tras encriptar los datos, el principio de estas tramas será el mismo, proporcionando un patrón que puede ayudar a los intrusos a romper el algoritmo de encriptación. Esto se soluciona utilizando un IV diferente para cada trama.

La vulnerabilidad de WEP reside en la insuficiente longitud del Vector de Inicialización (IV) y lo estáticas que permanecen las llaves de cifrado, pudiendo no cambiar en mucho tiempo. Si utilizamos solamente 24 bits, WEP utilizará el mismo IV para paquetes diferentes, pudiéndose repetir a partir de un cierto tiempo de transmisión continua. Es a partir de entonces cuando un intruso puede, una vez recogido suficientes tramas, determinar incluso la llave compartida.

En cambio, 802.11 no proporciona ninguna función que soporte el intercambio de llaves entre estaciones. Como resultado, los administradores de sistemas y los usuarios utilizan las mismas llaves durante días o incluso meses. Algunos vendedores han desarrollado soluciones de llaves dinámicas distribuidas.

A pesar de todo, WEP proporciona un mínimo de seguridad para pequeños negocios o instituciones educativas, si no está deshabilitada, como se encuentra por defecto en los distintos componentes inalámbricos.

3.2 OSA (Open System Authentication)

Es otro mecanismo de autenticación definido por el estándar 802.11 para autentificar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable.

3.3 ACL (Access Control List)

Este mecanismo de seguridad 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.

3.4 CNAC (Closed Network Access Control)

Este mecanismo 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.

4. MÉTODOS DE DETECCIÓN DE REDES INALÁMBRICAS

El método de detección de una red inalámbrica se denomina Wardriving y es bastante sencillo. Bastaría con la simple utilización de una tarjeta de red inalámbrica WNIC (Wireless Network Interface Card), un dispositivo portátil (ordenador portátil o incluso un PDA) con un software para verificar puntos de acceso y pasearse por un centro de negocios o algún sitio donde nos conste la utilización de una red inalámbrica. El ordenador portátil puede estar equipado con un sistema GPS para marcar la posición exacta donde la señal es más fuerte, o incluso una antena direccional para recibir el tráfico de la red desde una distancia considerable.

Una vez detectada la existencia de una red abierta, se suele dibujar en el suelo una marca con la anotación de sus características. Es lo que se denomina Warchalking, y cuya simbología se muestra a continuación:

SÍMBOLO	SIGNIFICADO
SSID)(Ancho de Banda	Nodo Abierto
SSID ()	Nodo Cerrado

SSID Contacto (W) Ancho de banda	Nodo WEP

Tabla 1: Simbología Warchalking

Por ejemplo el dibujo:

Xarxa
) (
1.5

Indicaría un nodo abierto, que utiliza el SSID Xarxa y que dispone de un ancho de banda de 1.5Mbps.

Esta simbología permite disponer de un mapa donde constan los puntos de acceso con sus datos (SSID, WEP, direcciones MAC,...). Si la red tiene DHCP, el ordenador portátil se configura para preguntar continuamente por una IP de un cierto rango, si la red no tiene DHCP activado podemos analizar la IP que figure en algún paquete analizado.

Existen varias herramientas útiles para detectar redes inalámbricas, las más conocidas son el AirSnort o Kismet para Linux y el NetStumbler para sistemas Windows.

Este mecanismo de detección de redes inalámbricas nos muestra lo fácil que es detectarlas y obtener información (incluso introducirnos en la red). A continuación se muestra un estudio realizado a fecha del 10 de Julio del 2002 en la ciudad de Manhattan:

APs	NÚMERO	PORCENTAJE
WEP INHABILITADO	198	75%
WEP HABILITADO	65	25%
TOTAL	263	100%

Tabla 2: Estadísticas Wardriving en la ciudad de Manhattan

Los estudios realizados indican un número elevado de redes inalámbricas sin el protocolo WEP activado o con el protocolo WEP activado pero con el SSID utilizado por defecto.

5. DISEÑO RECOMENDADO

Se podrían hacer varias recomendaciones para diseñar una red inalámbrica e impedir lo máximo posible el ataque de cualquier intruso.

Como primera medida, se debe separar la red de la organización en un dominio público y otro privado. Los usuarios que proceden del dominio público (los usuarios de la red inalámbrica) pueden ser tratados como cualquier usuario de Internet (externo a la organización). Así mismo, instalar cortafuegos y mecanismos de autentificación entre la red inalámbrica y la red clásica, situando los puntos de acceso delante del cortafuegos y utilizando VPN a nivel de cortafuegos para la encriptación del tráfico en la red inalámbrica.

Los clientes de la red inalámbrica deben acceder a la red utilizando SSH, VPN o IPSec y mecanismos de autorización, autenticación y encriptación del tráfico (SSL). Lo ideal sería aplicar un nivel de seguridad distinto según que usuario accede a una determinada aplicación.

La utilización de VPNs nos impediría la movilidad de las estaciones cliente entre puntos de acceso, ya que estos últimos necesitarían intercambiar información sobre los usuarios conectados a ellos sin reiniciar la conexión o la aplicación en curso, cosa no soportada cuando utilizamos VPN.

Como contradicción, es recomendable no utilizar excesivas normas de seguridad por que podría reducir la rapidez y la utilidad de la red inalámbrica. La conectividad entre estaciones cliente y PA es FCFS, es decir, la primera estación cliente que accede es la primera en ser servida, además el ancho de banda es compartido, motivo por el cual nos tenemos que asegurar un número adecuado de puntos de acceso para atender a los usuarios.

También se podrían adoptar medidas extraordinarias para impedir la intrusión, como utilizar receivers (Signal Leakage Detection System) situados a lo largo del perímetro del edificio para detectar señales anómalas hacia el edificio además de utilizar estaciones de monitorización pasivas para detectar direcciones MAC no registradas o clonadas y el aumento de tramas de reautentificación.

Por último también podrían ser adoptadas medidas físicas en la construcción del edificio o en la utilización de ciertos materiales atenuantes en el perímetro exterior del edificio, debilitando lo máximo posible las señales emitidas hacia el exterior. Algunas de estas recomendaciones podrían ser, aún a riesgo de resultar extremadas:

- Utilizar cobertura metálica en las paredes exteriores.
- Vidrio aislante térmico (atenúa las señales de radiofrecuencia).
- Persianas venecianas de metal, en vez de plásticas.
- Poner dispositivos WLAN lejos de las paredes exteriores.
- Revestir los closets (rosetas) de la red con un revestimiento de aluminio.
- Utilizar pintura metálica.
- Limitar el poder de una señal cambiando la atenuación del transmisor.

6. POLÍTICAS DE SEGURIDAD

Aparte de las medidas que se hayan tomado en el diseño de la red inalámbrica, debemos aplicar ciertas normas y políticas de seguridad que nos ayudarían a mantener una red más segura:

- Utilizar WEP, aunque sea rompible con herramientas como AirSnort o WEPCrack, como un mínimo de seguridad
- Utilizar mecanismos de intercambio de clave dinámica aportado por los diferentes productos comerciales hasta que el comité 802.11i, encargado de mejorar la seguridad en las redes inalámbricas, publique una revisión del estándar 802.11 con características avanzadas de seguridad, incluyendo AES (Advanced Encryption Standar) e intercambio dinámico de claves.
- Inhabilitar DHCP para la red inalámbrica. Las IPs deben ser fijas.
- Actualizar el firmware de los puntos de acceso para cubrir los posibles agujeros en las diferentes soluciones wireless.
- Proporcionar un entorno físicamente seguro a los puntos de acceso y desactivarlos cuando se pretenda un periodo de inactividad largo (ej. ausencia por vacaciones).
- Cambiar el SSID (Server Set ID) por defecto de los puntos de acceso, conocidos por todos. El SSID es una identificación configurable que permite la comunicación de los clientes con un determinado punto de acceso. Actúa como un password compartido entre la estación cliente y el punto de acceso. Ejemplos de SSID por defecto son “tsunami” para Cisco, “101” para 3Com, “intel” para intel,...
- Inhabilitar la emisión broadcast del SSID.
- Reducir la propagación de las ondas de radio fuera del edificio.
- Utilizar IPSec, VPN, firewalls y monitorizar los accesos a los puntos de acceso.

7. SISTEMAS DETECTORES DE INTRUSOS

Los sistemas detectores de intrusos, IDS, totalmente integrados en las redes clásicas cableadas, están tomando forma también en las redes inalámbricas. Sin embargo, aún son pocas las herramientas disponibles y sobretodo realmente efectivas, aunque empresas privadas están desarrollando y adaptando sus sistemas detectores de intrusos para redes inalámbricas (como ISS en su software Real Secure).

Las redes inalámbricas nos proporcionan cambios nuevos respecto a los sistemas de detección de intrusos situados en las redes clásicas cableadas.

En primer lugar, la localización de la estación capturadora del tráfico debe estar instalado en la misma área de servicios WLAN que queramos monitorizar. Este punto es crítico y obtendremos muchos falsos positivos si la localización es inapropiada o la sensibilidad del agente tan elevada que puede incluso capturar tráfico procedente de otras WLANs ajenas a la nuestra.

Otro punto crítico en los sistemas detectores de intrusos para redes es la identificación de tráfico anómalo, ya que existen aplicaciones como el NetStumbler y

Dstumbler que utilizan técnicas de descubrimiento de redes inalámbricas especificadas en 802.11 junto con otras propias, por lo que el agente IDS debe detectar y distinguir un tráfico de otro. Como punto positivo encontramos que ya existen patrones para distinguir a estos programas utilizados por los intrusos.

8. FUTUROS CAMBIOS: COMITÉ 802.11i

Siendo conscientes de las debilidades del estándar 802.11 en su protocolo WEP, se formó el comité 802.11i para paliar y mejorar los aspectos de seguridad en las redes inalámbricas. Muchos son los que creen que las medidas llegan tarde, y que las soluciones propietarias se han hecho 'dueñas' en este apartado mediante los protocolos ULA (Upper Layer Protocol), aplicables a las capas más altas del modelo OSI, y no especificadas en 802.11i por no ser objetivo del estándar.

8.1 LOS PROTOCOLOS ULA (Upper Layer Protocol)

Los protocolos ULA proporcionan intercambio de autenticación entre el cliente y un servidor de autenticación. La mayoría de los protocolos de autenticación incluyen:

- EAP-TLS (Extensible Authentication Protocol with Transport Layer Security), protocolo de autenticación basado en certificados y soportado por Windows XP. Necesita la configuración de la máquina para establecer el certificado e indicar el servidor de autentificación.
- PEAP (Protected Extensible Authetication Protocol), proporciona una autentificación basada en el password. En este caso, solamente el servidor de autentificación necesitaría un certificado.
- EAP-TTLS (EAP with Tunneled Transport Layer Security), parecido al PEAP, está implementado en algunos servidores Radius y en software diseñado para utilizarse en redes 802.11 (inalámbricas).
- LEAP (Lightweigh EAP), propiedad de Cisco y diseñado para ser portable a través de varias plataformas wireless. Basa su popularidad por ser el primero y durante mucho tiempo el único mecanismo de autenticación basado en password y proporcionar diferentes clientes según el sistema operativo.

Pero parece ser que nadie se escapa de la perspicacia de los intrusos, y cuando me encontraba redactando esta memoria me llegaba la noticia de un reciente ataque Man-in-the-middle a los protocolos PEAP y EAP-TTLS. Esto deja constancia de la rapidez con que se producen los cambios y de la inseguridad de algunas medidas adoptadas.

Las medidas que el comité 802.11i esta estudiando intentará mejorar la seguridad de las redes inalámbricas. Estas medidas se publicarán a principios de este año, pero ya existen documentos que nos hablan por donde se encaminan dichas mejoras.

Los cambios se fundamentan en 3 puntos importantes, organizados en dos capas.

A un nivel más bajo, se introducen dos nuevos protocolos de encriptación sobre WEP totalmente compatibles entre sí, el protocolo TKIP (Temporal Key Integrity Protocol) y el CCMP (Counter Mode with CBC-MAC Protocol), que trataré de explicar a continuación, junto con el estándar 802.1x para el control de acceso a la red basado en puertos.

8.2 ESTÁNDAR 802.1x

Como ya he comentado anteriormente, es un estándar de control de acceso a la red basado en puertos. Como tal, restringe el acceso a la red hasta que el usuario se ha validado.

El sistema se compone de los siguientes elementos:
- Una estación cliente.
- Un punto de acceso.
- Un servidor de Autenticación (AS).

Es este nuevo elemento, el Servidor de Autenticación, el que realiza la autenticación real de las credenciales proporcionadas por el cliente. El AS es una entidad separada situada en la zona cableada (red clásica), pero también implementable en un punto de acceso. El tipo de servidor utilizado podría ser el RADIUS, u otro tipo de servidor que se crea conveniente (802.1x no especifica nada al respecto).

El estándar 802.1x introduce un nuevo concepto, el concepto de puerto habilitado/inhabilitado en el cual hasta que un cliente no se valide en el servidor no tiene acceso a los servicios ofrecidos por la red. El esquema posible de este concepto lo podemos ver a continuación:

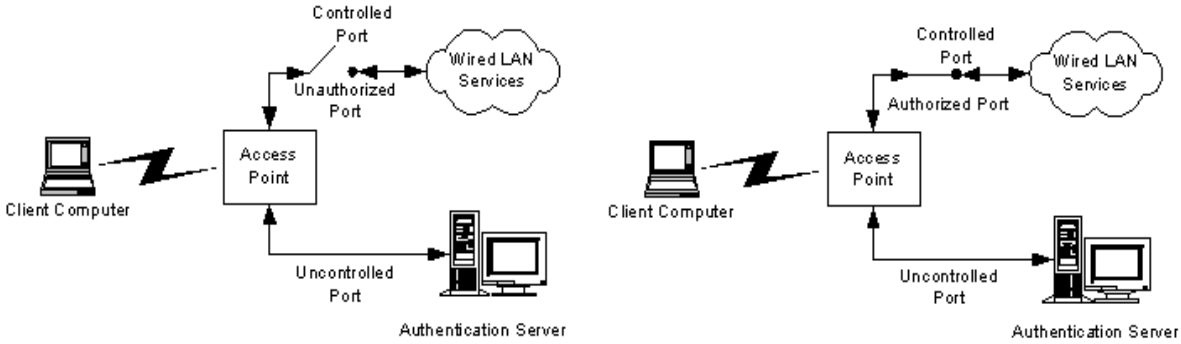

Figura 1: Esquema puerto habilitado/inhabilitado 802.1x

En sistemas con 802.1x activado, se generarán 2 llaves, la llave de sesión (pairwise key) y la llave de grupo (groupwise key). Las llaves de grupo se comparten por todas las estaciones cliente conectadas a un mismo punto de acceso y se utilizarán para el tráfico multicast, las llaves de sesión serán únicas para cada asociación entre el cliente y el punto de acceso y se creará un puerto privado virtual entre los dos.

El estándar 802.1x mejora la seguridad proporcionando las siguientes mejoras sobre WEP:
- Modelo de seguridad con administración centralizada.

- La llave de encriptación principal es única para cada estación, por lo tanto, el tráfico de esta llave es reducido (no se repite en otros clientes).
- Existe una generación dinámica de llaves por parte del AS, sin necesidad de administrarlo manualmente.
- Se aplica una autenticación fuerte en la capa superior.

8.3 TKIP (Temporal Key Integrity Protocol)

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP y mantener la compatibilidad con el hardware utilizado actualmente mediante una actualización del firmware.

El protocolo TKIP está compuesto por los siguientes elementos:

- Un código de integración de mensajes (MIC), encripta el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11. Esta medida protege contra los ataques por falsificación.
- Contramedidas para reducir la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.
- Utilización de un IV (vector de inicialización) de 48 bits llamado TSC (TKIP Sequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

La estructura de encriptación TKIP propuesta por 802.11i sería la siguiente:

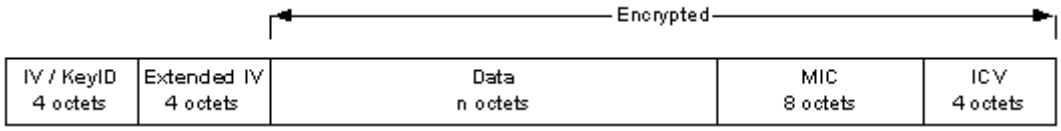

Figura 2: Estructura de encriptación TKIP

La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación. Pueden intercambiarse 2^{48} paquetes utilizando una sola llave temporal antes de ser rehusada.

En el proceso de encapsulación TKIP mostrada a continuación:

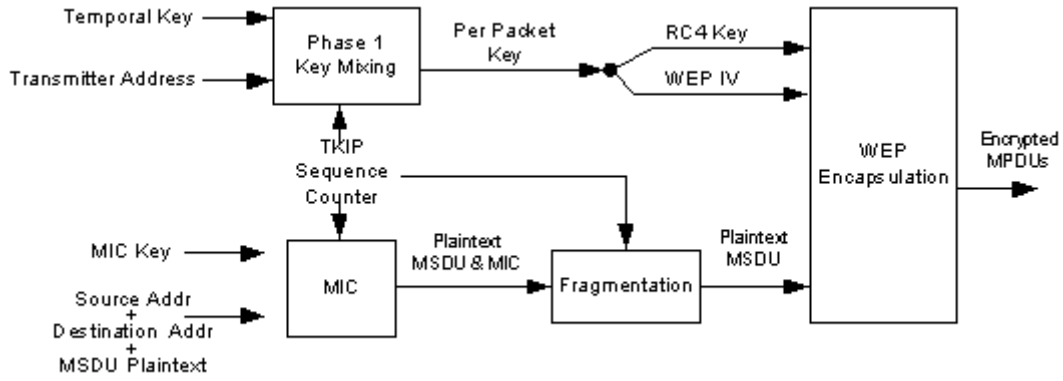

Figura 3: Proceso de encapsulación TKIP

Se combinan en dos fases la llave temporal, la dirección del emisor y el TSC para la obtención de una llave de 128 bits por paquete, dividido en una llave RC4 de 104 bits y en una IV de 24 bits para su posterior encapsulación WEP.

El MIC final se calcula sobre la dirección física origen y destino y el MSDU (MAC Service Data Unit o texto plano de los datos en la trama 802.11) después de ser segmentado por la llave MIC y el TSC.

La función MIC utiliza una función hash unidireccional, si es necesario, el MSDU se fragmenta incrementando el TSC para cada fragmento antes de la encriptación WEP.

En la desencriptación se examina el TSC para asegurar que el paquete recibido tiene el valor TSC mayor que el anterior. Sino, el paquete se descartará para prevenir posibles ataques por repetición. Después de que el valor del MIC sea calculado basado en el MSDU recibido y desencriptado, el valor calculado del MIC se compara con el valor recibido.

8.4 CCMP (Counter Mode with CBC-MAC Protocol)

Este protocolo es complementario al TKIP y representa un nuevo método de encriptación basado en AES (Advanced Encryption Standards), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC. Así como el uso del TKIP es opcional, la utilización del protocolo CCMP es obligatorio si se está utilizando 802.11i.

En la siguiente figura podemos observar el formato tras la encriptación CCMP:

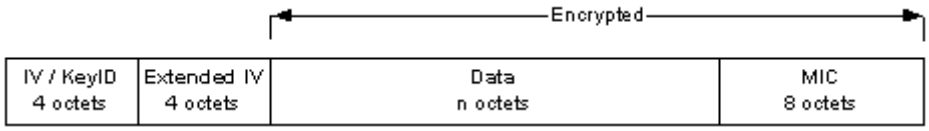

Figura 4: Estructura encriptación CCMP

CCMP utiliza un IV de 48 bits denominado Número de Paquete (PN) utilizado a lo largo del proceso de cifrado, junto con la información para inicializar el cifrado AES para calcular el MIC y la encriptación de la trama.

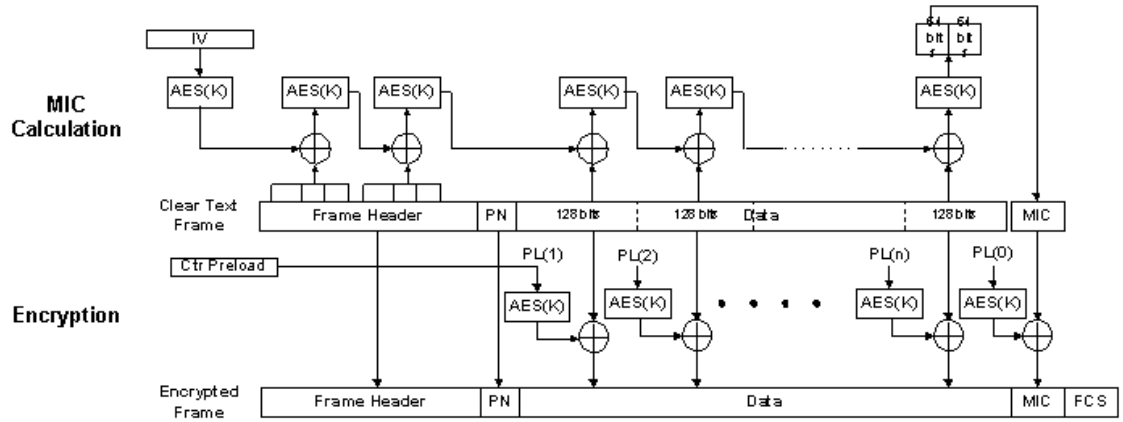

Figura 5: Proceso de encriptación CCMP

En el proceso de encriptación CCMP, la encriptación de los bloques utiliza la misma llave temporal tanto para el cálculo del MIC como para la encriptación del paquete. Como en TKIP, la llave temporal se deriva de la llave principal obtenida como parte del intercambio en 802.1x. Como podemos observar en la figura 5, el cálculo del MIC y la encriptación se realiza de forma paralela. El MIC se calcula a partir de un IV formado por el PN y datos extraídos de la cabecera de la trama. El IV se convierte en un bloque AES y su salida a través de la operación XOR conformará el siguiente bloque AES.

9. CONCLUSION

Con la tecnología inalámbrica se nos abre todo un mundo de posibilidades de conexión sin la utilización de cableado clásico, proporcionando una flexibilidad y comodidad sin precedentes en la conectividad entre ordenadores.

Esta tecnología tiene como mayor inconveniente la principal de sus ventajas, el acceso al medio compartido de cualquiera con el material y los métodos adecuados, proporcionando un elevado riesgo de seguridad que tendremos que tener presentes a la hora de decantarnos por esta opción y que crecerá en igual medida (o más rápido) que las soluciones aportadas para subsanar estos riesgos.

Por lo tanto se recomienda la utilización de una política de seguridad homogénea y sin fisuras, que trate todos los aspectos que comporten riesgo, sin mermar la rapidez y que sepa aprovechar las ventajas de las redes inalámbricas.

ANEXO A: Herramientas de Auditoría

ESCÁNERS WLAN

NOMBRE	PLATAFORMA	WEBSITE
NetStumbler	Windows	www.NetStumbler.org
Dstumbler	BSD	www.dachb0den.com/projects/dstumbler.html
MacStumbler	Macintosh	http://homepage.mac.com/macstumbler
MiniStumbler	Pocket PC	www.NetStumbler.org
SSIDSniff	Unix	www.bastard.net/~kos/wifi
Airosniff	Unix	http://gravitino.net/~bind/code/airosniff
AP Scanner	Macintosh	http://homepage.mac.com/typexi/Personal1.html
Wavemon	Linux	www.jm-music.de/projects.html
WLAN Expert	Windows	www.vector.kharkov.ua/download/WLAN/wlanexpert.zip
Wavelan-tools	Linux	http://sourceforge.net/projects/wavelan-tools
Kismet	Linux, iPaq, Zaurus	www.kismetwireless.net
AiroPeek	Windows	www.wildpackets.com/products/airopeek
Sniffer Wireless	Windows	www.sniffer.com/products/sniffer-wireless
TCH-WarDrive	Linux	www.thehackerschoice.com
APSniff	Windows	www.bretmounet.com/APSniff
Wellenreiter	Linux	www.remote-exploit.org
PrismStumbler	Linux	http://prismstumbler.sourceforge.net
AirTraf	Linux	http://airtraf.sourceforge.net

SNIFFERS WLAN

NOMBRE	PLATAFORMA	WEBSITE
Mognet	Java VM	http://chocobospore.org7mognet
Kismet	Linux, iPaq, Zaurus	www.kismetwireless.net
Ethereal	Unix, Windows	www.ethereal.com
TCPDump	Unix	www.tcpdump.org
PrismDump	Unix	http://developer.axis.com/download/tools
Prism2Dump	BSD	www.dachb0den.com/projects/prism2dump.html
AiroPeek	Windows	www.wildpackets.com/products/airopeek
Sniffer Wireless	Windows	www.sniffers.com/products/sniffer-wireless

WEP KEY CRACKERS

NOMBRE	PLATAFORMA	WEBSITE
WEPCracker	Perl	http://sourceforge.net/projects/wepcrack
AirSnort	Linux	www.be-secure.com/airsnort.html
AirSnort for BSD	BSD	www.dachb0den.com/projects/bsd-airsnort.html

BIBLIOGRAFÍA

http://neworder.box.sk
www.80211-planet.com
www.commsdesign.com
www.hispasec.com
www.ebcvg.com
http://standards.ieee.org/getieee802/802.11.html
www.valenciawireless.org
www.madridwireless.net
www.drizzle.com/~aboba/IEEE/
www.personaltelco.net
www.securitywireless.info