POLITICAS DE SEGURIDAD PARA REDES INALAMBRICAS

Lady Mariana Molano Rodriguez y Doris Emilse Cubillos Pinilla
Universidad Piloto de Colombia, Facultad de Ingeniería,
Especialización en Seguridad Informática Bogotá, Colombia
ing.marianam@hotmail.com
emilsecubillos@hotmail.com

Abstract - The effective managing of the resources of the wireless network is important for the benefit Of the users of our network and the Institution. The effective, ethical, moral and legal use of the resources of the wireless network is important For the benefit of the users of our network and the Institution. This document describes how the wireless technology will be used, administered, Assured and supported. Also he assures that all the users of the wireless network should receive a level of Quality service as for reliability, integrity, availability of service and Safety. It complements Procedures for the Ethical Legal Use of the Technologies of Information including specific actions to the network Wireless and to the resolution of situations that could suggest.

Palabras Claves - Políticas de Seguridad, WEP, Protocolos, Estándar 802.11, TKIP

I. INTRODUCCION

La flexibilidad y la movilidad que nos proporcionan las nuevas redes inalámbricas han hecho que la utilización de estas redes se haya disparado como el mejor método para realizar conectividad de datos en edificios sin necesidad de cablearlos.

Pero como todas las 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 las ondas de radio como un medio de transmisión.

Por esta razón se 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.

II DEFINICION

Una red inalámbrica es un conjunto de computadoras interconectadas entre sí, por medio de ondas de radio (Wireless).

El objetivo de construir una red consiste en que todas las computadoras que forman parte de ella se encuentren en condiciones de compartir su información y sus recursos con las demás. De esta manera, se estaría ahorrando dinero, debido a que si se colocara un dispositivo, por ejemplo, una impresora, todas las computadoras de la red podrían utilizarlo.

III REGLAMENTO PARA EL USO DE LA RED INALAMBRICA

Artículo 7: De modo que exista seguridad en el uso de la red se contara con las siguientes disposiciones:

- El acceso a la infraestructura de la red, incluyendo la infraestructura inalámbrica está limitada a personas autorizadas a usar los recursos de Internet de la Universidad.
- Debe ser mantenida una seguridad física con la finalidad de evitar el robo de los equipos o el acceso a los puertos de datos.
- La infraestructura inalámbrica punto a punto o multipunto no proporciona codificación autenticación. El passwords y la protección de los datos es responsabilidad de la aplicación utilizada por el equipo Inalámbrico para suministrar Internet Inalámbrico.

- Los puntos de acceso deben utilizar autentificación de usuarios y además restringir la aceptación de la conexión mediante la verificación de la dirección MAC de los computadores.

IV RIESGOS DE LAS REDES INALAMBRICAS

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 sería 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.

V. POLÍTICAS DE SEGURIDAD

Además de las medidas que se han tomado en el diseño de la red inalámbrica, se deben aplicar ciertas normas y políticas de seguridad las cuales ayuden 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 passwords 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.

VI. 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.

VIII FUTUROS CAMBIOS: COMITÉ 802.11i

Con previo conocimiento de que el estándar 802.11 contiene debilidades en su protocolo WEP, se formó el comité 802.11i para atenuar 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.

A. 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 Manin-the-middle a los protocolos PEAP y EAPTTLS. 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 está estudiando intentarán mejorar la seguridad de las redes inalámbricas. Estas medidas se publicarán a principios de este año, pero ya existen documentos que nos hablan por dónde 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 Integrista 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.

B. Estándar 802.1x

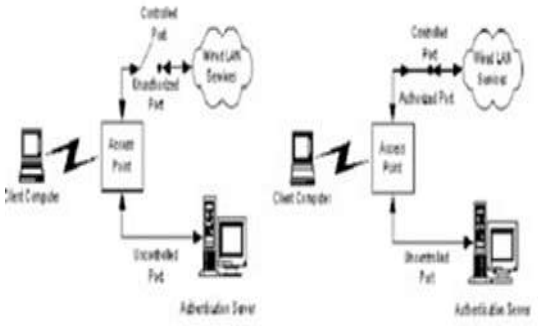
Es un estándar de control de acceso a la red basado en puertos que restringe el acceso a la red hasta que el usuario se ha validado.
El sistema se compone de los siguientes elementos:

- 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:

Fig. Esquema puerto habilitado/inhabilitado 802.1x



Fuente:www.uv.es/~montanan/ampliacion/trabajos/SeguridadWireless.pdf

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.

C. 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:

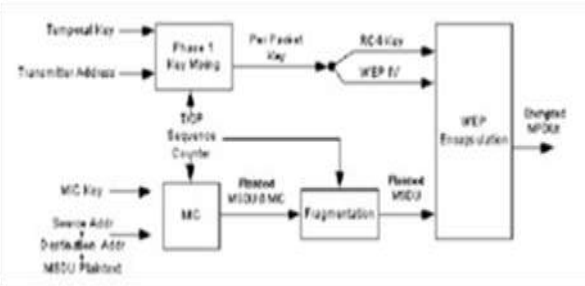
- Un código de integración de mensajes (MIC), encripta el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11. Esta medida protege contra los ataques por falsificación.
- Contramedidas para reducir la probabilidad de que un atacante 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:

Fig: Estructura de encriptación TKIP

Fuente:www.uv.es/~montanan/ampliacion/trabajos/SeguridadWireless.pdf

La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de re decodificar la llave temporal durante una sola asociación. Pueden intercambiarse 248 paquetes utilizando una sola llave temporal antes de ser rehusada.
En el proceso de encapsulación TKIP mostrada a continuación:

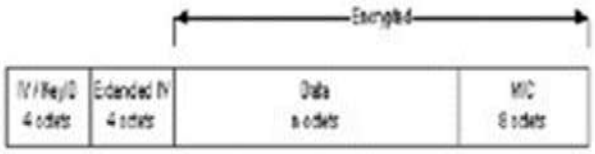
Fig: Proceso de encapsulación TKIP

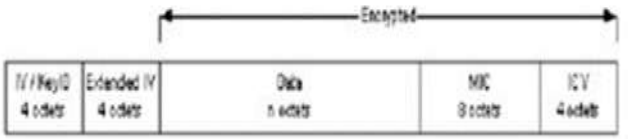


Fuente:www.dspace.espol.edu.ec/bitstream/123456789/5613/4/Seguridad%20en%20Redes%20Inal%C3%A1mbricas.pdf

Se combina 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 des encriptado, el valor calculado del MIC se compara con el valor recibido. 8.4 CCMP (Counter Mode with CBC-MAC Protocol)

Fig: Estructura encriptación CCMP





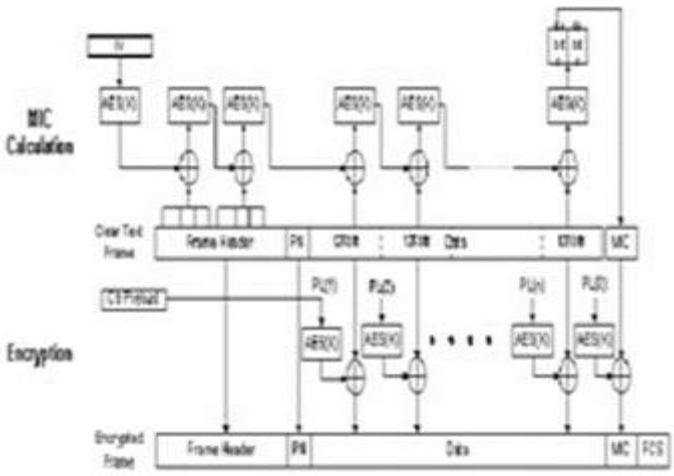
Fuente: www.cert.uy/historico/pdf/Seguridad_en_wifi.pdf

Este protocolo es complementario al TKIP y representa un nuevo método de encriptación basado en AES (Advanced Encryption Standarts), cifrado simétrico que utiliza bloques de 28 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 inscripción 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.

Fig: Proceso de encriptación CCMP

Fuente:www.cert.uy/histórico/PDF/Seguridad_en_wifi.pdf



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.

IX CONCLUSIONES

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

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 disminuir la rapidez y que sepa aprovechar las ventajas de las redes inalámbricas.

REFERENCIAS BIBLIOGRAFÍCAS

- Política de Uso y Seguridad de la Red Inalámbrica, Wilberto Vega Rivera, Mayo 2007
- Reglamento de la Red Inalambrica, Instituto de Estudios Superiores de Chiapas
- Seguridad en redes Inalámbricas, Universitat de Valencia, Vicent Alapont Miquel
- www.personaltelco.net
- www.securitywireless.info
- www.80211-planet.com
- www.commsdesign.com
- www.hispasec.com
- www.cert.uy/historico/pdf/Seguridad_en_wifi.pdf
- www.uv.es/~montanan/ampliacion/trabajos/SeguridadWireless.pdf