ENTENDIENDO LAS WIRELESS LAN

AciD-KrS (acidkrs@kernelpanik.org)

Murcia (15/02/2002) - Part. I

INDICE

1. Introducción
    a. Capa física FHSS.
        i. Estándar 802.11a
    b. Capa física DSSS.
        i. Estándar 802.11b.
    c. Capa MAC.

2. Topología.
    a. Redes Ad-Hoc (Punto a Punto).
    b. Redes de Infraestructura.

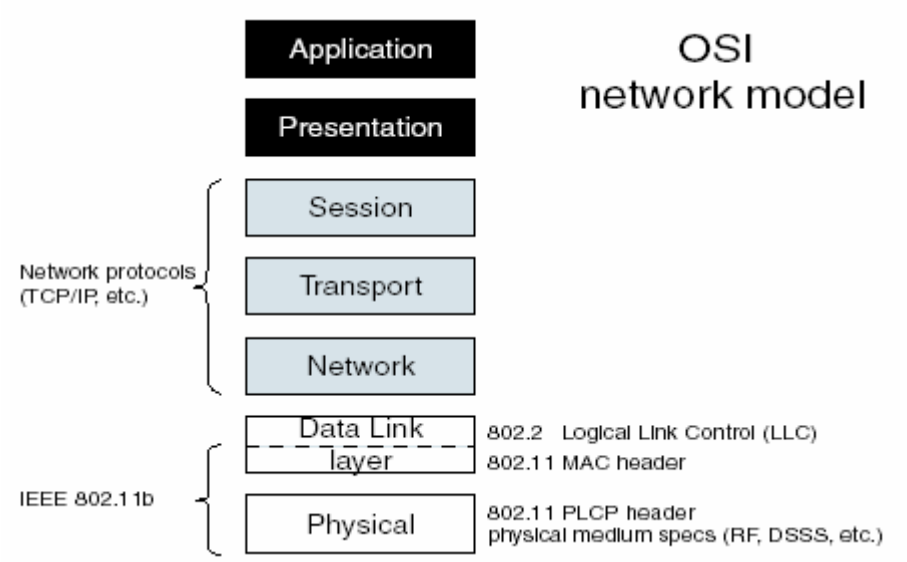
3. Mecanismos de seguridad.
    a. Autenticación abierta.
    b. Autenticación "shared key".
    c. Autenticación cerrada.
    d. Listas de control de acceso. (ACLs).
    e. Manejo de llaves. (Key management).

4. Protocolo WEP.
    a. Atacando el keystream.
    b. Atacando los mensajes.
        i. Desencriptar.
            1. Redirección IP.
            2. Ataques de reacción.
        ii. Inyectar.

1. Introducción

En la actualidad, se esta masificando la implantación del estándar 802.11 para ámbitos empresariales, docentes e incluso domésticos llevando consigo una gran libertad de movimiento en las comunicaciones. Este sistema de comunicación lleva consigo una serie de ventajas respecto a las redes alambicas, pero a la vez un peligro potencial si existe una mala configuración o se comete el gran error de dejar los valores predeterminados por cada fabricante, puesto que dejaría expuesta la red interna a cualquier persona armada con un simple portátil, una Wireless Card y por ejemplo, el conocido AirSnort para capturar los datos que circulen por esta red. Como nota a destacar, recientemente miembros del Chaos Computer Club (CCC) grabaron y publicaron un video sobre la inseguridad de estas redes en universidades alemanas que podréis ver en la web del grupo Hispahack (hispahack.ccc.de).

En 1999, el IEEE (Institute of Electrical and Electronics Engineers) aprobó el 802.11 y define los protocolos de comunicación inalámbrica para redes locales. Específicamente, describe la funcionalidad de las capas de acceso (MAC) y física (PHY). El principal objetivo del servicio descrito en el estándar 801.11 es la entrega de unidades de datos (MSDU - MAC Service Data Units) entre unidades de control lógico de conexión (LLC - Logical Link Controls).



La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos. En la capa física, se definen dos métodos de transmisión RF y un infrarrojo. El funcionamiento de la WLAN en bandas RF ilícitas, requiere la modulación en banda ancha para reunir los requisitos del funcionamiento en la mayoría de los países. Los estándares de transmisión RF en el estándar, son la Frecuencia de Saltos (FHSS: Frecuency Hopping Spread Spectrum) y la Secuencia Directa (DSSS: Direct Sequense Spread Spectrum). Ambas arquitecturas se definen para operar en la banda de frecuencia de 2.4 GHz, ocupando típicamente los 83 MHz de banda desde los 2.400 GHz hasta 2.483 GHz. (DBPSK: Differential BPSK) y DQPSK es la modulación para la Secuencia Directa. La tasa de datos de la capa física para sistemas FHSS es de 1Mbps. Para DSSS se soportan tanto tasas de datos de 1 Mbps como de 2 Mbps. La elección entre FHSS y DSSS dependerá de diversos factores relacionados con la aplicación de los usuarios y el entorno en el que el sistema esté operando.

En vista de esto, el IEEE estableció 2 grupos de trabajo para explotar este estándar.

Grupo A: El nuevo estándar 802.11a trabaja en un espectro de 5,15 – 5,35GHz a 5,725-5,825GHz, con cuatro canales independientes y tasas de transferencia de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

Grupo B: Estándar que actualmente está en el mercado. Define la operación en un espectro de frecuencias de entre 2,4 y 2,4835 GHz y soporta tres canales independientes con tasas de transferencia de 1, 2, 5,5 y 11 Mbps, en función de la distancia y de la claridad de la señal. La modulación utilizada para este estándar se conoce como DSSS (Direct Sequence Spread Spectrum).

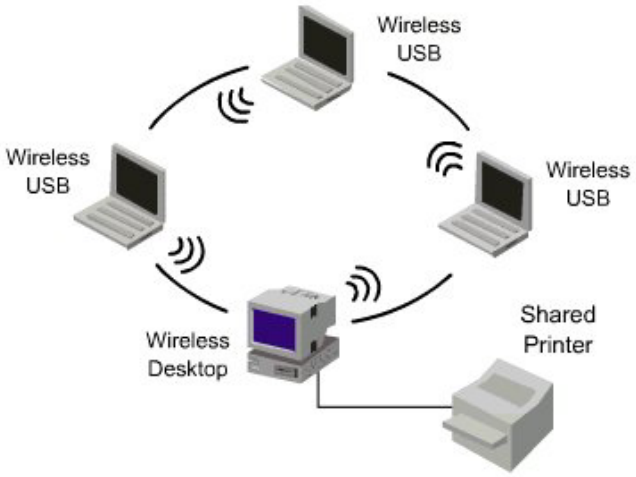
La Capa MAC tiene similitudes a la de Ethernet (802.3) cableada usando el protocolo CSMA/CA para la detección de colisiones, pero en este tipo de redes descubrir dichas colisiones son difíciles y se anula. Otro factor importante es determinar si un canal esta vacío, para este fin se utiliza un algoritmo de estimación de desocupación de canales o lo que es lo mismo CCA, el cual realiza una medición de la energía RF de la antena y determina la fuerza de la señal recibida, denominada RSSI.

2. Topología.

Depende de la funcionalidad con la que se desee montar este tipo de redes, se puede hacer de 2 modos distintos: Ad-Hoc o lo que es lo mismo, redes punto a punto o bien por infraestructura.

Redes Ad-Hoc (Punto a Punto).

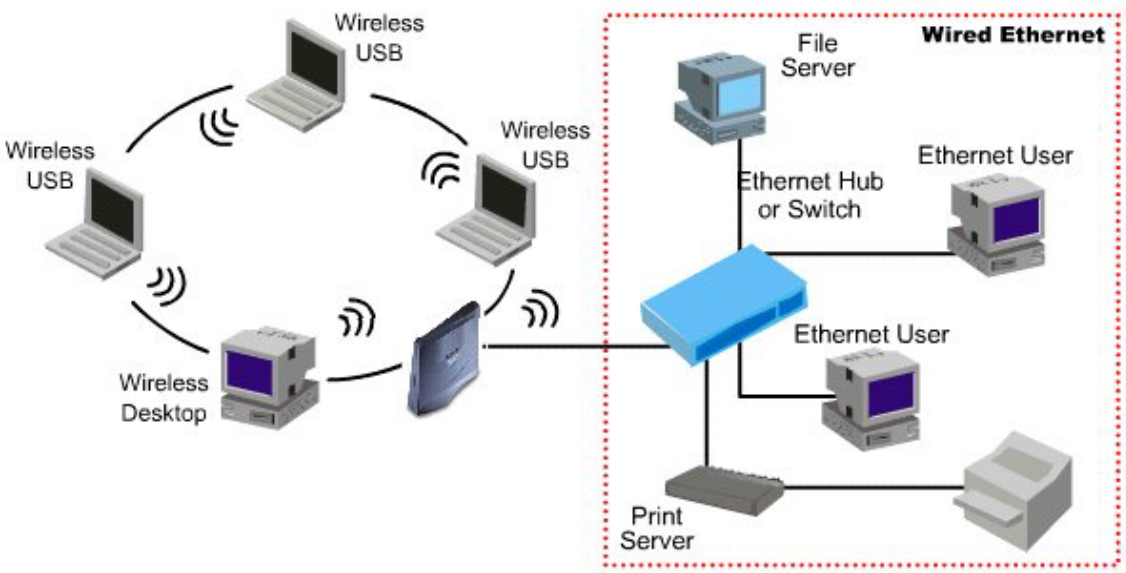
El estándar denomina a este modo como un servicio básico independiente (IBSS) con un coste bajo y flexible. Las comunicaciones entre los múltiples nodos se establecen sin el uso de ningún servidor u otro medio como pueden ser los puntos de acceso o Access Point (AP) .



Uno de los métodos básicos para encaminar paquetes en este modo, seria tratando a cada uno de los nodos que forman la red como un router y utilizando entre ellos un protocolo convencional (como puede ser los basados en el vector de distancia) para encaminarlos hacia su destino.

Redes de infraestructura.

En este modo, cada cliente de la red envía todas sus comunicaciones a una central o punto de acceso (AP, Access Point). Para efectuar el intercambio de datos, previamente los clientes y los puntos de acceso establecen una relación de confianza.



Los APs, pueden emplearse dentro de la Wireless Lan como:

a. Gateway: para redes externas (Internet, intranet, etc.).
b. Bridge: hacia otros Access Points para extender los servicios de acceso.
c. Router: de datos entre el área de cobertura, abarcando los 100-150mts en un entorno cerrado (dependiendo de la disposición y objetos que bloqueen las ondas de radio) o los 300mts en espacios abiertos.

a.

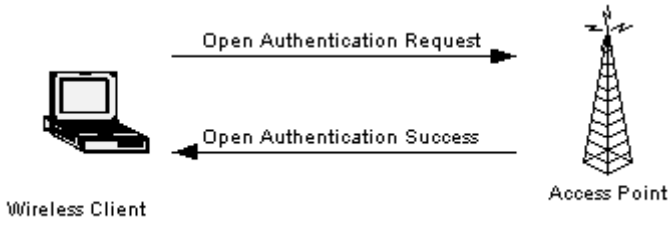
Estos puntos de acceso tienen un límite de 64 NICs (Network Interface Cards) dentro de su área de actuación. Para paliar este problema se opta por poner en funcionamiento varios APs al mismo tiempo, ampliando así las posibilidades de roaming de un equipo móvil sin perder la conexión.

3. Mecanismos de seguridad.

El proceso de conexión del cliente a la red comienza cuando el cliente hace un barrido de todas las frecuencias usadas por 802.11b enviando su dirección MAC (Dirección física) y el ESSID (Extended Set Service ID), siendo este último el nombre de la red a la que deseamos acceder. Todos los APs en el rango responderán con su propio ESSID, canal y dirección MAC. Con esta información, el cliente puede limitar su señal y comenzar el proceso de autenticación.

Autenticación abierta.

Es el protocolo por defecto para las redes 802.11. Todos los clientes que inician el proceso de autenticación ante un AP son registrados en la red. Ambos, envían en texto plano todos los *management frames,* incluso cuando el WEP (Wireless Encription Protocol) está activado.



Vulnerabilidades

El propio sistema es una vulnerabilidad en sí mismo, absolutamente todos los clientes que piden ser autenticados en la red lo son.

Autenticación "Shared Key"

Se basa en un desafío cliente <---> Access Point, en donde ambos comparten una llave secreta para iniciar dicha autenticación, siendo el cliente el dispositivo móvil que desea ser autentificado y el AP (también conocido como "responder") el que recibirá dicha petición.

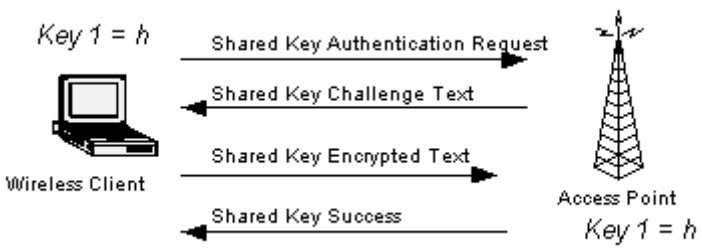
El cliente, envía una trama (management frame) indicando que el método a usar es de llave compartida. Al recibir el AP esta trama, enviará una nueva con los 128 Bytes de texto para ser usado como desafío. Estos Bytes se generan por el PRNG (Pseudo-Random Number Generator) usando dicha llave y un vector de inicialización (IV – Initialization Vector).

Una vez recibida esta segunda trama por el cliente, se copia el contenido del desafío en el cuerpo de una nueva trama, que a su vez es encriptada con WEP usando la llave compartida mas un nuevo vector de inicialización (esta vez es elegido por el cliente). Una vez realizado todo esto se envía al *responder.*

El Access Point al recibir esta trama procede a:

a. Desencriptarla.
b. Comprobar si el CRC es válido.
c. Verificar la validez del *desafío.*

Una vez realizado este proceso de manera satisfactoria, el AP autentifica al cliente. Una vez completado este paso, se realiza de manera inversa. De esta manera se produce una autenticación mutua y el cliente es registrado en la red.



Vulnerabilidades

Mediante un analizador de red, es fácil obtener los datos necesarios para recrear tramas válidas y *engañar* al Access Point al que se desea conectar. Capturando el segundo mensaje, obtendríamos el *texto desafío* aleatorio en texto plano y con el tercer mensaje el mismo texto pero ya encriptado y el vector de inicialización.

Autenticación cerrada

Sistema basado en el Extended Service Set ID (ESSID) de cada Access Point. Es un código alfanumérico que esta incluido en todos los APs y en los clientes que participan dentro de la misma wireless.

Este sistema es usado por los equipos móviles como PDAs, etc. los cuales para acceder a la red de servicios de dicho fabricante (por ejemplo 3com) llevan ya grabados dicho código.

Vulnerabilidades

Cada fabricante establece valores por defecto que no son modificados por administradores inexpertos.

Cisco Systems : tsunami.
3com : 101.
Agere : WaveLan network.

Listas de control de acceso. (ACLs)

Estas listas están confeccionadas con las direcciones físicas de cada cliente, es decir su dirección MAC. Cada Access Point establecerá que direcciones son válidas para permitir la unión de un cliente a su red. Muchos de los fabricantes de los APs distribuyen herramientas de configuración que ayudan al administrador a confeccionar dichas listas.

Vulnerabilidades

Las direcciones físicas viajan en texto plano y con un analizador de red, se pueden capturar las direcciones permitidas por dicho AP. Modificando la NIC (Network Interface Card), un intruso puede acceder a dicha red.

Manejo de llaves. (Key management)

Son 4 el número de llaves que pueden ser guardadas en la capa de enlace (para el modelo llave compartida). Estas llaves no pueden ser utilizadas directamente, sino que forman parte de una solución de capas más altas (del modelo OSI).

4. Protocolo WEP.

El cifrado es una manera habitual de implementar seguridad y protección en los datos. WEP aplica un conjunto de instrucciones, llamado *algoritmo a la información* cuyas instrucciones combinan texto en *claro* con una secuencia de números hexadecimales, llamada clave de cifrado.

Las redes inalámbricas compatibles con 802.11b incorporan tecnologías de Wired Equivalent Privacy (WEP). Existen dos métodos de cifrado WEP:

a. 64 (40) Bits.
b. 128 Bits.

Una clave de 64 (40) bits consiste en 10 números hexadecimales distribuidos en dos grupos de cinco dígitos:

a. Clave No. 1: 10111 21314
b. Clave No. 2: 20212 22324
c. Clave No. 3: 30313 23334
d. Clave No. 4: 40414 24344

Y de 128 Bits basada en 26 números hexadecimales distribuidos en dos grupos de cinco dígitos y cuatro grupos de cuatro dígitos:

a. Clave No. 1: 10111 21314 1516 1718 191A 1B1C
b. Clave No. 2: 20212 22324 2526 2728 292A 2B2C
c. Clave No. 3: 30313 23334 3536 3738 393A 3B3C
d. Clave No. 4: 40414 24344 4546 4748 494A 4B4C

Atacando el KeyStream.

El principal problema reside en la propia implementación de este algoritmo (RC4), cuyo keystream es generado en función del vector de inicialización (v) y una llave (k) la cual esta almacenada en la NIC y en el Access Point.

WEP encripta basándose en el siguiente algoritmo:

$$C = (T) \text{ xor } (RC4(v,k))$$

C Texto encriptado
T Texto original + CRC de 32 Bits.

Este ataque fue ideado por Nikita Borisov, Ian Goldberg, y David Wagner de la universidad de Berkeley. Considerando previamente:

a. C1 = P1 XOR RC4(v,k)
b. C2 = P2 XOR RC4(v,k)

Y lo llevaron acabo de la siguiente forma:

$$C1 \text{ XOR } C2 = (P1 \text{ XOR } RC4(v,k)) \text{ XOR } (P2 \text{ XOR } RC4(v,k)) = P1 \text{ XOR } P2$$

Obteniendo el texto cifrado mediante :

$$P \text{ XOR } C = P \text{ XOR } (P \text{ XOR } RC4(v,k)) = RC4(v,k)$$

Atacando los mensajes.

- **Desencriptando el tráfico:** Una escucha pasiva, puede interceptar todo el tráfico que pasa por la red hasta la colisión del IV. Con un XOR de dos paquetes que tengan el mismo vector, un atacante puede obtener el XOR de los dos mensajes en texto plano, pudiendo ser utilizado para deducir datos sobre el contenido de dichos mensajes. Cuando el análisis estadístico es poco concluyente (basado solamente en dos mensajes), el atacante puede buscar más colisiones con el mismo vector de inicialización. Con un poco de tiempo, es posible recuperar un número considerable de mensajes cifrados, aumentando el índice de éxito del análisis. Una vez sea posible recuperar el texto plano entero para uno de los mensajes, los siguientes pueden ser obtenidos también directamente, puesto que todas las parejas de XOR son conocidas.

  En algunos casos, el atacante intenta redirigir los paquetes hacia una de las maquinas en Internet a la cual tiene acceso. Para ello solo le basta cambiar en la cabecera del paquete la dirección de destino. Cuando dicho paquete llega al Access Point, es desencriptado y enviado a la nueva dirección.

- **Inyectando tráfico: Para** dicho fin, el atacante debe conocer el texto del mensaje sin cifrar. Basándose en este conocimiento es posible generar paquetes cifrados correctos, para ello basta con calcular el CRC-32 y utilizar el *bit flip* del mensaje original para cambiar el texto del nuevo mensaje. Una vez construido, se envía al Access Point o a otro nodo de la red y será validado como paquete válido.

  Una modificación leve a este ataque lo hace mucho más insidioso. Incluso sin el conocimiento completo del paquete, es posible modificar valores en un mensaje y ajustar con éxito el CRC cifrado. Si el atacante tiene conocimiento parcial del contenido de un paquete, puede interceptarlo y realizar la modificación selectiva. Por ejemplo, es posible alterar los comandos que se envían a una shell en una sesión del telnet.