Seguridad en redes inalámbricas IEEE 802.11

Criptografía y seguridad de redes

Jose Manuel Morales
David Hontecillas

Indice

Introducción

En la actualidad el uso de las Redes de Área Local (LAN) está ampliamente extendido.

Las redes LAN actuales sufren una serie de inconvenientes:
-coste de desplegar la red (cableado, equipos),
-impacto de la instalación de esta
-falta de flexibilidad.

El siguiente paso ha consistido en el diseño de las WLAN, o Redes de Área Local Inalámbricas. Estas redes proporcionan la conveniencia de las LAN tradicionales, pero sin los inconvenientes mencionados. En este caso hablaremos del caso particular de la familia de estándares 802.11 del IEEE.

Formatos

de igual a igual (*peer-to-peer*) Dos equipos se comunican directamente sin necesidad de un equipo intermedio que haga de repetidor.

con infraestructura. (caso más común) El equivalente a las LAN tradicionales, constan de un Punto de Acceso (AP) que conecta una LAN tradicional ya existente con los equipos que hacen uso de la WLAN.

Seguridad en el estándar IEEE 802.11

- Veremos los mecanismos de seguridad especificados en el estándar 802.11.
- Las redes actualmente usadas se basan en el estándar 802.11b, que es un anexo al 802.11 en donde se definen los requerimientos para la implementación de WLAN a una velocidad de hasta 11 Mbps, operando en la banda libre de frecuencias de 2.4 GHz, también se especifica el uso de modulación de espectro ensanchado, así como la disponibilidad de hasta 14 canales.

Mecanismos de Seguridad

- El estándar 802.11 define una serie de mecanismos básicos que tienen como objetivo proporcionar una seguridad equivalente a la de una red tradicional cableada. Para ello buscamos dos objetivos básicos:
- **Autentificación**: el objetivo es evitar el uso de la red (tanto en la WLAN como la LAN a la que conecta el AP) por cualquier persona no autorizada. Para ello, el Punto de Acceso solo debe aceptar paquetes de estaciones previamente autentificadas.
- **Privacidad**: consiste en encriptar las transmisiones a través del canal radio para evitar la captura de la información. Tiene como objetivo proporcionar el mismo nivel de privacidad que en un medio cableado.
- Con estos objetivos en mente se definen los mecanismos básicos de 802.11. Posteriormente se han observado deficiencias en estos mecanismos que los debilitan, y debido a ello se han desarrollado nuevos mecanismos, adicionales o en sustitución de los anteriores, como veremos posteriormente.

Conexión a la red

- Cuando un dispositivo desea conectarse a una red WLAN, primero debe conocer el SSID (*Service Set ID*). Este actúa como un identificador de la red. En el estándar 802.11 se especifica que este identificador se retransmitir en difusión (*broadcast*) cada pocos segundos, anunciando de esta forma la red. Esto permite la conexión de clientes de manera sencilla, pero a su vez permite la identificación de redes sin dificultad.
- Los vendedores de equipos dan a este parámetro un valor por defecto que suele ser conocido, como es el caso de *tsunami* por parte de Cisco, o *WaveLAN network* por parte de Agüere. Una primera medida de seguridad consiste en modificar el parámetro para que tenga otro valor, preferiblemente uno que no tenga ninguna relación con la red.

Autentificación

- Para poder hacer uso de la red una vez conectado a ella es necesario que la estación se autentifique con el punto de acceso.
- Tanto para el uso de la red inalámbrica[1] como para el acceso a la red convencional a la que esté conectada la primera, en caso que esto suceda.

- 802.11 especifica dos tipos de autentificación:

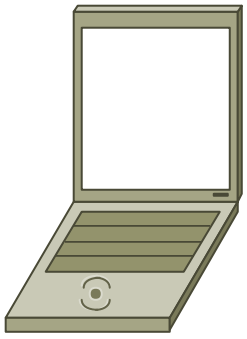
  -autentificación abierta

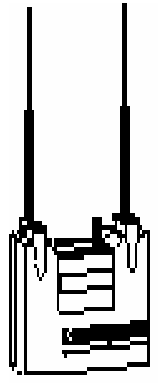
  Simplemente se acepta a cualquier estación

  -autentificación por clave compartida.

  La clave compartida usada es la misma que la clave que se usa para la encriptación **WEP**. Para autentificar una estación, el AP envía un desafío en texto claro a la estación, que esta devuelve encriptado usando la clave compartida. A su vez el AP también realiza la misma operación, y compara ambos resultados. En caso de que ambos coincidan se permite el acceso a la estación

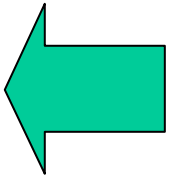
- [1] Esto es debido a que en el caso de las redes con infraestructura toda comunicación a través de esta pasa por el AP, independientemente de si el destino de la transmisión se encuentra en la misma red o en otra.

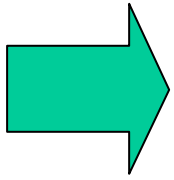




AP

Secreto Compartido





Challenge (Nonce)

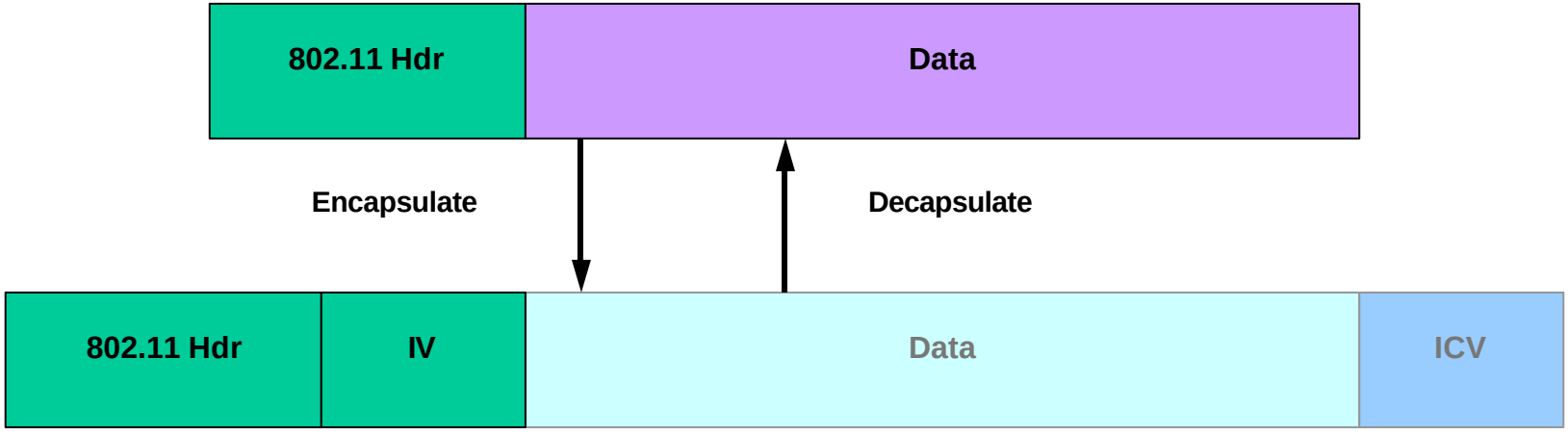
Respuesta (Nonce RC4 encriptado bajo llave compartida)

Decrypted nonce OK?

Privacidad

- Para proporcionar privacidad en redes 802.11 se usa WEP (*Wired Equivalent Privacy* o Privacidad Equivalente al Cable). Este protocolo es el que encripta los paquetes de datos en texto claro antes de su transmisión por el canal. Para ello se usa el cifrado RC4.
- Cada paquete se encripta con una clave distinta, que consiste en la concatenación de el campo IV (que viaja en texto claro en el paquete) junto con la clave compartida WEP. La longitud del campo IV es de 24 bits (hay por tanto 16,8 millones de combinaciones posibles para encriptar un paquete con una misma clave WEP), mientras que la longitud de la clave WEP es de 40 bits, sumando un total de 64 bits para encriptar el paquete. Hay que notar, pero, que la clave WEP según la especificación de 802.11 es **estática**. Esto conlleva una serie de problemas que veremos más adelante.

- En la figura vemos el formato del paquete, que en el caso de que esté encriptado mediante WEP solo se realiza esta operación sobre los campos de datos e ICV. Este último consiste en un CRC de 32 bits para comprobar la integridad de los datos.
- Es importante destacar que la implementación de WEP es **opcional** según el estándar, y por ello inicialmente no se implementó en muchos equipos.



Amenazas y debilidades

Amenazas a la conexión

- Debido al hecho de que el SSID se está difundiendo en el aire cada pocos segundos es muy simple para un atacante descubrir una red. Sólo hace falta escuchar el medio por unos instantes para detectar en que canales se está operando una WLAN y el nombre de la misma.
- Es por ello que una de las primeras medidas tomadas por un fabricante para mejorar la seguridad de la red fue por parte de Lucent en sus equipos Orinoco WaveLAN, y consistió en lo que vinieron a llamar Red Cerrada (*Closed Network*). Esta red cerrada consistía simplemente en no anunciar la red mediante el frame de *beacon*, o sea, no hacer difusión del SSID.
- Hoy en día esta medida es simplemente una dificultad añadida para el atacante, que debe tomar algún esfuerzo adicional para descubrir la red. Como veremos más adelante existen sniffers en la actualidad como AirSnort o AirTraf que pueden descubrir estas redes sin la menor dificultad.

Amenazas a la autentificación

- La autentificación por clave compartida envía el desafío en texto claro por el canal. Así mismo, el desafío encriptado se devuelve por el mismo canal. Por tanto, usando un ataque de fuerza bruta se puede tratar de descubrir la clave compartida. Así un atacante puede llevar a cabo un ataque pasivo sin ser detectado para descubrir la clave secreta, debido a que el canal se propaga sin control por parte de los participantes legítimos de la red.
- Una vez descubierta la clave secreta el atacante tiene acceso a la red, Podrá encriptar-desencriptar todo el tráfico, debido a que la clave de autentificación es la misma clave de encriptación WEP.Pasando ser un usuario más en la red.
- Una de las soluciones a este problema vino de la mano de Lucent, con la encriptación WEP de 128 bits (WEP Plus). Con ella, la clave compartida pasa de 40 a 104 bits, haciéndola más resistente al anterior ataque.
- Adicionalmente hay personas que creen que es más seguro desactivar la autentificación usando este protocolo, ya que de esta forma se puede proteger más la clave.

- A partir de octubre de 2000 aparecieron una serie de documentos donde se describían las vulnerabilidades de WEP, y de las redes 802.11. [3] Entre ellas, la presentación “Overview of 802.11 Security” [4] pone de manifiesto las vulnerabilidades de la encriptación WEP, **usando cualquier longitud de clave**.
- Se demuestra en el documento que, debido a que WEP usa un IV (*Initialisation Vector*) de 24 bits, por la paradoja del aniversario únicamente con 4823 paquetes ya hay una probabilidad de colisión del 50%, o sea, de que se repita el mismo IV.
- Dado que RC4 realiza la encriptación de los valores usando un XOR del mismo con un byte pseudo aleatorio, podemos ver que dos bytes de dos flujos de datos cualquiera, usando el mismo IV y encontrándose en la misma posición relativa dentro de estos flujos tendrán los valores:

$$c_1 = p_1 \oplus b \qquad\qquad c_2 = p_2 \oplus b$$

- Siendo c1 el byte cifrado, p1 el byte en texto claro y b el byte pseudo aleatorio. En este caso vemos que, uniendo ambos bytes cifrados podemos, aún sin saber la clave, obtener la siguiente información:

$$c_1 \oplus c_2 = (p_1 \oplus b) \oplus (p_2 \oplus b) = p_1 \oplus p_2$$

- Usando esta información y sabiendo informaciones clave dentro del paquete (por ejemplo, el formato de la cabecera IP que viaja en la mayoría del tráfico en las redes actuales), podremos intentar un ataque pasivo contra la red. Adicionalmente, mediante el ICV, que viaja también cifrado en el paquete, podremos saber si la desencriptación del mismo se ha llevado a cabo correctamente.

- Debido a que IV sea tan corto esta vulnerabilidad se manifiesta independientemente de la longitud de la clave (40 o 104 bits). Usando WEP de 128 bits ciertamente se dificulta la desencriptación de los paquetes, pero seguimos teniendo el problema de la colisión de valores IV. Adicionalmente, se puede intentar forzar tráfico en la red atacada para reducir el tiempo necesario para que se produzca esta colisión.
- También se describe la vulnerabilidad de la encriptación RC4 en el documento “Weaknesses in the Key Scheduling Algorithm of RC4” [5].
- Este ataque se ha llevado a la práctica en el programa AirSnort [1], que permite, escuchando la red atacada, recuperar la clave WEP. Citando su página, podemos ver que únicamente se requieren del orden de 5 a 10 millones de paquetes para llevar a cabo el ataque. Una vez obtenidos los paquetes necesarios, la clave se puede recuperar en menos de un segundo.
- Realizando algunos cálculos podemos ver que en redes corporativas este tráfico puede obtenerse en uno o dos días sin demasiados problemas. Es por tanto que una de las principales soluciones viene dada por la rotación de las claves WEP, o la asignación dinámica de las mismas, de forma que nunca se llegue a obtener la información suficiente para poder romper la clave.

3.Tecnologías específicas

- **Filtrado de direcciones MAC**

  Una de las primeras medidas llevadas a cabo fue el filtrado de direcciones MAC dejado pasar únicamente el tráfico de las tarjetas con dirección MAC conocida.

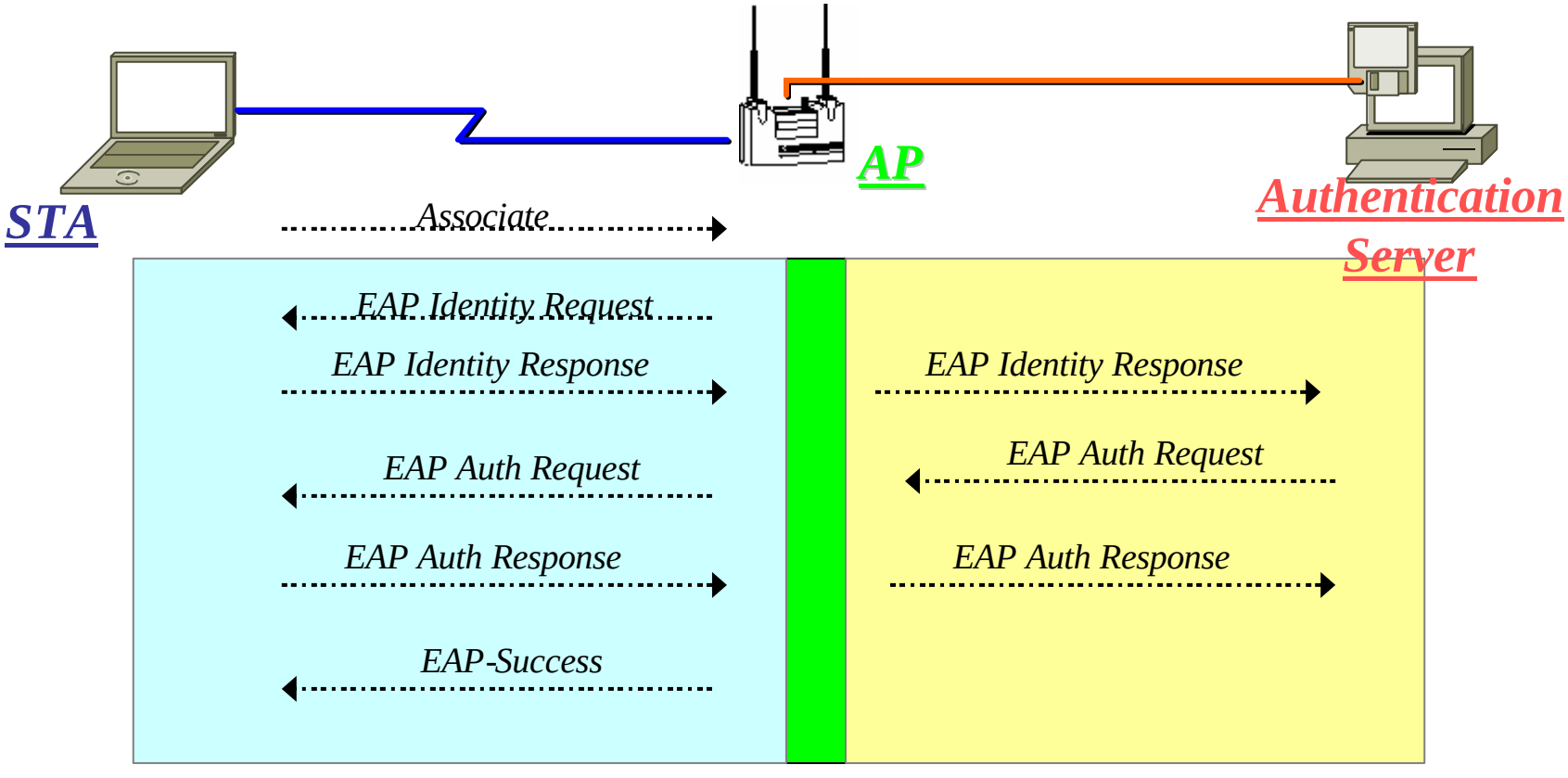
En la práctica:

- **Dificultad de administración**: el administrador de la red debe disponer de una lista de direcciones admitidas, e irlas actualizando en cada uno de los AP (o bien instalar un servidor RADIUS para mantener la lista).
- **Falsa seguridad**: es muy sencillo modificar la dirección MAC de una tarjeta de red. Debido a que la dirección MAC no viaja encriptada por WEP, es muy sencillo para un atacante escuchar en la red para obtener una lista de direcciones MAC válidas, y luego simplemente cambiar la dirección de su tarjeta para usar cualquiera de ellas.
- Por tanto, esta medida simplemente puede proporcionar una cierta dificultad adicional a un atacante, pero en ningún momento constituye una solución de seguridad por si misma.

El estándar 802.1x

- Especifica los mecanismos necesarios para llevar a cabo un control de acceso por puerto en redes 802. Este estándar, ha tenido una gran aceptación , y su implementación está disponible en varias formas por parte de los fabricantes.
- 802.1x define el control de acceso por puerto. Para ello, cuando un dispositivo quiere acceder a una red a través de un AP, este solicita unas credenciales al mismo. Esta solicitud se realiza usando EAP (*Extensible Authentication Protocol*). Una vez recibidas las credenciales por parte de la estación, el AP reenvía las mismas a un servidor de autentificación RADIUS, que realiza la autentificación del usuario y autoriza su acceso.
- Debido a que EAP es un protocolo genérico, puede transportar diferentes tipos de autentificación, con diferentes prestaciones cada uno de ellos.

802.1X Model


STA
AP
Authentication Server
Associate
EAP Identity Request
EAP Identity Response
EAP Identity Response
EAP Auth Request
EAP Auth Request
EAP Auth Response
EAP Auth Response
EAP-Success

EAP-MD5

- En el caso de EAP-MD5 se utiliza un hash MD5 del nombre de usuario y su clave para llevar a cabo la autentificación. Debido a ello, no existe peligro en este sentido de usar la autentificación para poder romper la clave WEP.
- Adicionalmente, debido a que la autentificación es por usuario, existen más posibilidades de restringir el uso de la red para usuarios concretos, sin la necesidad de tener que cambiar la clave WEP en todos los AP y todas las estaciones.
- EAP-MD5 no ofrece ninguna prestación adicional.

EAP-TLS

- EAP-TLS ha sido desarrollada por Microsoft, y viene implementada en Windows XP. También existen clientes para otras versiones (excepto Windows CE) y para Linux.
  EAP –TLS usa certificados X.509 para llevar a cabo la autentificación, en lugar de nombres de usuario y palabras clave. Por ello, es necesario un servidor de certificados para poder hacer uso de esta autentificación. Además, es necesario poder expedir los certificados necesarios, o poder comprar los mismos a una autoridad certificadora. Por tanto, la única forma sencilla de uso de EAP-TLS es mediante el Microsoft Certificate Server haciendo uso de Active Directory para mantener las claves. Todo ello conlleva la necesidad de la instalación de los servidores necesarios y el aprendizaje del manejo de la plataforma. Por tanto, este tipo de autentificación solo es adecuada para empresas medianas o grandes, y usando por el momento únicamente la plataforma de Microsoft.

Ventajas de EAP-TLS

Se dialoga sobre TLS, que es la estandarización de SSL

Autentificación de ambas partes

Uso de claves WEP dinámicas y de un solo uso

Asignación para cada sesión de las claves, un usuario legítimo de la red no podrá interceptar tráfico de otro usuario

Imposición de autentificación cada pocos minutos, de forma que vuelve totalmente imposible el ataque pasivo. Esto es gestionado de manera transparente al usuario.

EAP-TTLS

- Creada por Funk Software, EAP-TTLS es similar a EAP-TLS con algunas modificaciones. Mientras que el AP se sigue autentificando mediante un certificado, la estación usa un nombre de usuario y clave, que transmite usando cualquier mecanismo de autentificación estándar (PAP, CHAP, MS-CHAP, PAP/Token Card o EAP). El AP usa un servidor RADIUS para comprobar la autenticidad del usuario y permitirle el acceso. Es algo menos seguro que EAP-TLS, aunque más sencillo de implementar.

PEAP

- PEAP son las siglas de Protected EAP, un protocolo desarrollado conjuntamente por Microsoft y Cisco como una alternativa a EAP-TLS. Este protocolo usa TLS y certificados para realizar el transporte de la información de autentificación, pero esta se realiza usando MS-CHAP v2. Por tanto, únicamente se requiere un único certificado X.509 para TLS, sin necesidad de un certificado por usuario. La autentificación se hace mediante usuario y clave directamente a un servidor RADIUS, sin necesidad de disponer de un servidor de certificados. Asi se mantiene un alto nivel de seguridad pero no se requiere una infraestructura de clave pública como en el caso de EAP-TLS, reduciendo costes.
- Al igual que EAP-TLS, PEAP dispone de clave WEP dinámica.

Debilidades 802.1x

- 802.1x fue diseñado para redes cableadas.
- En el documento “An Initial Security Analysis of the IEEE 802.1X Protocol” [6] se describe un ataque de hombre en el medio (*man-in-the-middle*) que permite desviar todo el tráfico a un AP atacante.
- Este ataque se puede llevar a cabo incluso para el caso de EAP-TLS, que proporciona autentificación fuerte de ambas partes, tanto la estación como el AP.
- La base de este ataque viene dada por el hecho de que EAP no proporciona mecanismos de autentificación del mensaje. El ataque entonces consiste básicamente en iniciar una autentificación y realizar el envío de un paquete EAP Success falso por parte del atacante, que indica que la autentificación ha sido correcta. Esto hace creer a la estación que ha iniciado realmente una sesión con el AP, permitiendo que la estación inicie el envío de tráfico hacia el atacante.

FUTURO INMEDIATO EL ESTÁNDAR 802.11i

- 802.11i es el estándar propuesto para la seguridad futura de las WLAN. También conocido como RSN (*Robust Security* Network), o en sus implementaciones pre-estándar como WPA (*WiFi Protected Acess*), se basa en 802.1x para proporcionar una seguridad adicional a este. Este protocolo promete sustituir al WEP en lo que a encriptación de los paquetes se refiere. Para ello usa AES en modo OCB.
- Además, se varía el formato de la trama para evitar los problemas de WEP. Entre ellos, usa in IV de 128 bits y encripta únicamente los datos, junto con un número de secuencia. De esta forma se evita la debilidad que proporciona el que ICV de encuentre encriptado, ya que de esta forma se puede comprobar fácilmente que se dispone de la clave correcta comprobando que ICV concuerda.
- Actualmente WPA no se encuentra disponible por parte de los fabricantes, pero van apareciendo primeras implementaciones, y se espera que el número de los equipos que lo soporten crezca en cuanto finalmente el IEEE apruebe el estándar 802.11i para finales del tercer trimestre de este año.

Conclusiones

- Inicialmente 802.11, debido al momento en que se desarrolló (la seguridad no era tan necesaria y las leyes de exportación de EEUU restringían la exportación de criptografía de clave fuerte), era inseguro.
- Con el tiempo se han ido realizando mejoras sobre el protocolo inicial. Primeramente se dificultó la detección de las redes y se aumentó la longitud de clave para proporcionar mayor protección.
- Posteriormente, viendo que el diseño inicial era inherentemente inseguro, se decidió usar 802.1x para la autentificación, proporcionando una autentificación mucho más segura, y permitiendo el uso de claves WEP dinámicas, otro de los errores de diseño del protocolo.
- Finalmente en la actualidad está en proceso de estandarización el IEEE 802.11i, que promete una seguridad mucho mayor, sumándole a las características de 802.1x una encriptación fuerte mediante AES.

Un ejemplo de vulnerabilidad

- WI-FI utiliza el protocolo CSMA/CA y MACA
  - MACA Multi Access Collision Avoidance
  - Antes de TX el emisor envia un RTS con long de datos a TX
  - El Recpetor envia un CTS repitiendo long
  - Al recibir CTS se envia.

  - ATAQUE DOS
  - El atacante modifica su soft para que en cuanto escuche un RTS envie un CTS.
  - Se Produce colision las unidades se desconectan

Referencias

- [1] *AirSnort*, http://airsnort.shmoo.com/
- [2] *AirTraf*, “Leaving the randomness out of wireless site surveys”, L. Victor Marks, http://www-106.ibm.com/developerworks/wireless/library/wi-airtraf/
- [3] *802.11 Security Vulnerabilities*, Collage Park, http://www.cs.umd.edu/~waa/wireless.html
- [4] *Overview of 802.11 Security*, Jesse Walker, http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3-Overview-of-802-11-Security.ppt
- [5] *Weaknesses in the Key Scheduling Algorithm of RC4*, Scott Fluhrer, Itsik Mantin and Adi Shamir. Presentado al “Eighth Annual Workshop on Selected Areas in Cryptography”, August 2001. http://downloads.securityfocus.com/library/rc4_ksaproc.pdf http://www.crypto.com/papers/others/rc4_ksaproc.ps
- [6] *An Initial Security Analysis of the IEEE 802.1X Protocol*, Arunesh Mishra, William A. Arbaugh, http://www.cs.umd.edu/~waa/1x.pdf
- Referencias adicionales:
- *Ars Technica Wireless Security Blackpaper*, Trey "Azariah" Dismukes, http://www.arstechnica.com/paedia/w/wireless/security-1.html
- *Microsoft Solution for Securing Wireless LANs*, http://www.microsoft.com , sección de “Downloads”