B I N A R I A

¿SON INSEGURAS LAS REDES LAN INALÁMBRICAS?

Dipl. Ing. Johann Haag
Director del departamento Redes de comunicación

Dipl. Ing. (FH) Gerald Kraushofer

En los últimos años la sociedad exige mucha más flexibilidad y movilidad a las personas. Han surgido nuevos conceptos de oficina; el lugar de trabajo "fijo" en muchas empresas ha pasado a formar parte del pasado. Con estas demandas adicionales aumentan naturalmente también las expectativas sobre los equipos IT. Por esta razón, la red inalámbrica parecería la solución ideal para muchos usuarios, de no ser por la cantidad de artículos publicados que tratan sobre los riesgos en cuestión de seguridad. Muchos departamentos IT incluso rechazan la instalación de redes Lan inalámbricas en sus empresas. Como muestran las cifras de venta y los estudios correspondientes [John Cumbers Networkers 2003], alrededor del 40% de las redes Lan inalámbricas instaladas no son implementadas por el departamento IT, sino por los usuarios, que quieren aprovechar estas nuevas posibilidades. Este trabajo pretende analizar los problemas de la inseguridad de las redes Lan inalámbricas. De cualquier manera dado que las redes "seguras" no son más que desiderata, vamos a explicar los riesgos en seguridad, así como, las posibles medidas para luchar contra ellos y compararlos con los riesgos de las redes "clásicas".

Definiciones/Destinatarios:

Los autores de este artículo parten de la base de que el lector está familiarizado con los conceptos básicos de la comunicación con redes de datos, y por eso se presupondrán conocimientos sobre los mecanismos para el acceso al control de las redes inalámbricas y los protocolos usados.

Como el concepto de seguridad desde nuestro punto de vista no está claramente definido en los libros queremos definir los puntos más relevantes comparamos redes inalámbricas y redes convencionales (véase. Fuhrberg Kai, 2000, p.54 sig.):

1) Confidencialidad: No se puede ni visualizar ni interpretar los datos sin la autorización debida.
2) Integridad: No es posible la modificación no autorizada o inadvertida de los datos o de información de los sistemas
3) Disponibilidad: los procesos deben ejecutarse en un momento y un plazo de tiempo determinados.

El riesgo de virus y gusanos no serán tomados en consideración, ya que es obvio que no hay ninguna diferencia entre las redes inalámbricas y las convencionales

Métodos de Ataque

Los métodos de ataque pueden diferenciarse entre ataques pasivos y ataques activos.

1) Ataques pasivos

En los ataques pasivos no se ataca la red, sino que discretamente se accede a la red y se analiza la circulación de datos. Este tipo de ataques sirven para espiar información como Direcciones IP, contraseñas, etc, y en muchas ocasiones sirven como preparación para un ataque activo (véase. Planet 3 Wireless 2002, P. 282 sig.).
Los ataques más peligrosos se pueden dividir de la siguiente manera:

i. Port Scanning: (escaneo de puertos) como todos los protocolos TCP (Protocolo de control de transmisión) y UDP (Protocolo de datagramas de usuario) que ofrece el ordenador los ofrece por, es muy útil para espiar el número de puerto usado. Así se puede a través de un número de puerto evitar la función del Firewall para atacar más tarde de forma activa. El Port Scanning (Escaneado de puertos) funciona de tal manera que el atacante envía datos con distintos números de puerto al ordenador "escaneado". Como con cada TCP se responde a cada petición de acceso, si es necesario se responderá con un mensaje de error y el atacante puede espiar los puertos.

ii. Sniffing: Aquí el atacante necesita una entrada a la red. Por medio de un analizador de protocolos (ej. Ethherreal, Sniffer…) se graban y analizan todos los datos. Estos ataques son muy difíciles de llevar a cabo en redes convencionales, ya que se necesita o bien un acceso directo o una red interna (Ataque de colaborador), o grabar y analizar todos los datos de un segmento a través de conexión a Internet.
En las redes LAN inalámbricas este acceso es más sencillo, ya que las ondas electromagnéticas también pueden recibirse desde el exterior del edificio. Si los datos no están codificados el "fisgón" puede escuchar y grabarlos fácilmente los datos.

2) Ataques Activos

Si el hacker ya ha obtenido suficiente información a través de los ataques pasivos puede atacar la red de forma directa y cambiar los datos, y parar el sistema. Estos ataques tienen como objetivo dañar la integridad y la disponibilidad del sistema (véase. Kai Fuhrberg, 2000, p. 62 sig.)

I. Spoofing (engaño):
IP Spoofing (engaño de IP): Muchos privilegios en la red se gestionan por medio de direcciones IP inequívocas. El atacante puede acceder a los datos si ha encontrado las direcciones.
DNS Spoofing (engaño de DNS): El *Domain Name System*, sistema de referencia/información en Internet, que se encarga de trasladar las direcciones que se detectan fácilmente (ej. www.fh-stpoelten.ac.at) a las direcciones IP correspondientes (198.15.13.12). Cuando el usuario introduce una dirección de este tipo en el navegador origina en un segundo plano una petición en el servidor DNS. Este servidor DNS, a su vez, memoriza las direcciones por

servidores superiores, es decir, por peticiones anteriores. Ya que el servidor DNS no comprobó la veracidad de los datos, también graba la información falsa que le proporciona un atacante. El usuario es enviado a un servidor falso, y no se da cuenta del ataque, ya que casi nunca conoce la dirección IP correspondiente.
MAC Spoofing (de engaño de MAC): Al igual que con IP Spoofing, aquí se utiliza una dirección MAC conocida de un usuario para poder fingir una identidad falsa.

II. Ataques Jamming (ataque denegación de servicio): El atacante intenta parar la red o un sólo ordenador, mediante un número elevado de peticiones. Para hacerlo utiliza fallos de protocolo. (Ej.: TCP SYN Flooding) (véase Planet 3 Wireless 2002, p. 285)

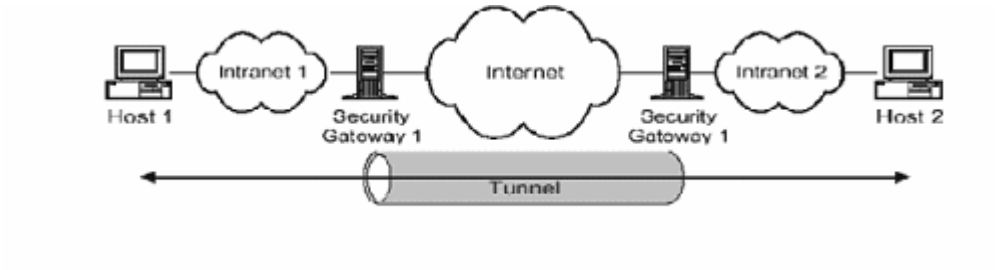
III. Ataques Man-in-the.middle (ataque de intercepción): El atacante se interpone y finge ser usuario y servidor al mismo tiempo. Estos ataques son especialmente peligrosos ya que el atacante obtiene toda la información necesaria sobre los certificados de seguridad, etc
Este peligro es muy elevado sobre todo en redes LAN inalámbricas. El cliente siempre intenta conectarse desde el Punto de Acceso (Access Point, AP) que disponga de la señal más fuerte, por eso resulta normal que se cambie al AP que disponga de la emisión más potente. Por tanto, si se acepta un AP "falso", quizás incluso con una potencia de emisión demasiado alta, todos los clientes se cambiarán a la señal del atacante y transferirán todos sus datos a través de esta nueva vía. Para el atacante se vuelve muy sencillo filtrar los datos que le interesan. Por supuesto el AP tiene que estar configurado (SSID,…) de antemano en el AP "correcto".

IV. Perturbación de la banda de frecuencia a través de un interferente: Las redes LAN inalámbricas se pueden interrumpir muy fácilmente activando un emisor con una mayor potencia. Estos ataques suelen afectar sobre todo a la disponibilidad de las redes.

En los próximos párrafos se presentan las distintas posibilidades de protección. Ya que los sistemas Firewall se conciben principalmente para separar y proteger las redes privadas de las públicas, y que no se establece ninguna diferencia por el tipo de acceso a la red, tampoco las vamos a analizar aquí.

VPN

Los VPN (Virtual Private Network) se utilizan para unir dos componentes de una red por medio de una red insegura. A través de esta red se intercambian datos privados. En este punto es donde normalmente interviene el VPN, al conectar, por medio de Internet, redes o puestos de trabajo remotos a la red local de la empresa. El puesto de trabajo remoto, es decir, el cliente, puede ser un ordenador de consola, un portátil, un PDA o cualquier hardware que utiliza la puerta de enlace de una red privada virtual.
Una red Lan inalámbrica representa así mismo –parecido a Internet- una red insegura y puede clasificarse en la misma categoría de seguridad que un acceso RAS (Remote Access Service). Por eso puede utilizarse también un VPN en las redes LAN inalámbricas para proteger los datos transferidos. Para la transmisión de los datos se crea un túnel y todos los datos que pasen por dicho túnel estarán codificados.



Existen un gran número de protocolos de túnel. Los más importantes son el L2TP (Layer 2 Tunneling Protocol, Protocolo de Túnel de capa 2) y el IPSec (IP Security Protocol, Protocolo de Seguridad IP).

L2TP

El IETF (Grupo de Trabajo de Ingeniería de Internet) ha desarrollado el protocolo L2TP que es una combinación del protocolo PPTP y del protocolo L2F (Layer 2 Forwarding) desarrollado por Cisco, el L2TP combina las ventajas de los protocolos que lo forman. El protocolo L2TP en Windows ya no utiliza el MPPE (Microsoft Point-to- Point Encryption, Protocolo de encriptación de punto a punto de Microsoft), cuando utiliza el IPSec. Es decir, que en las conexiones VPN basadas en L2TP se usa una combinación de L2TP y una IPSec. También son posibles los protocolos IP, IPX (Internet Work Packet Exchange, Intercambio de paquetes de Internet), etc… [2]

IPSec

El IPSec ha sido desarrollado por la IETF y, a diferencia de las soluciones anteriores, representa un estándar. El protocolo consta de dos partes, una parte se encarga de la codificación de los datos y la otra parte de asegurar su integridad y autenticidad. El primer componente de la IPSec es ESP (Carga de Seguridad Encapsulada) que se encarga de la codificación, para la que se pueden emplear distintos procedimientos de encriptación. El segundo componente se denomina AH (Cabecera de autentificación) que impide la manipulación de los datos.
El protocolo IKE (Intercambio de claves de internet) no es un componente de las IPSec; sin embargo, está estrechamente vinculado a él, es el encargado de la gestión de claves.
La IPSec ha demostrado ser un protocolo seguro; hasta la fecha no ha podido ser pirateado. (véase Hein, 2002, p. 801 sig.)

Posibles protecciones para las redes LAN inalámbricas

Encriptación WEP

En la norma IEEE 802,11 para redes LAN inalámbricas está definido el uso del protocolo WEP (véase. norma IEEE 802,11 de 1999, p. 41). El protocolo WEP está basado en un algoritmo de encriptación simétrico que tiene un código secreto. Este código secreto lo tienen grabado tanto el cliente como el Punto de Acceso. Con esta clave secreta y un vector de inicialización (VI) se generará a través de un Pseudo Random Number Generador (PRNG) una secuencia de bits aleatoria. Para el PRNG se utiliza un algoritmo de cifrado RC4. El vector inicial ha de transferirse como texto sin codificar, ya que sirve para inicializar el PRNG. Como el cifrado WEP no está implementado con un gestor de claves tiende a utilizarse la misma clave durante un largo periodo de tiempo. Es justo aquí donde empiezan

los puntos débiles. Como el vector inicial tiene 24 bit se crean un total de 2^{24}=16777216 posibilidades hasta que se repita el VI. Si el atacante conoce el texto sin cifrar (ya sea por haber causado un fallo o por promedios estadísticos) (véase Networkers 1) podrá piratear la clave.
Por tanto, el cifrado WEP no es seguro al cien por cien. Scott Fluhrer, Itisk Mantin y Adi Ahamir analizaron estos puntos débiles y publicaron sus trabajos bajo el título: *Puntos débiles en el algoritmo generador de claves RC4* (véase RC4 2). Basándose en estos trabajos se publicaron, poco después, programas (ej. Airsnort) con los que sin grandes conocimientos se pueden craquear claves secretas.

Las posibilidades actuales de proteger las redes LAN inalámbricas con encriptación WEP no son suficientes dado a los puntos débiles que contiene y que han sido descritos. Tanto los fabricantes de sistemas LAN inalámbricos, como las distintas organizaciones normalizadotas de estándares intentan eliminar estos problemas con medidas de seguridad alternativas e implementaciones adicionales. Las siguientes alternativas de seguridad son unas de las medidas más efectivas para utilizar los sistemas LAN inalámbricos de una forma segura.

A través de la inserción de VPN se pueden eludir los puntos débiles del WEP. Sin embargo, el inconveniente es que debido al exceso de trabajo que ocasiona la encriptación VPN el rendimiento se ve mermado.

VPN para redes LAN inalámbricas

El túnel VPN acaba siempre en el servidor VPN, es decir, una puerta de enlace VPN. El sistema VPN puede estar formado de distintas maneras:

- Existen AP (Puntos de Acceso), que ya tienen integrado un servidor VPN. Esta variante se utiliza a menudo en pequeñas y medianas empresas, en las que la autentificación se realiza, bien, consultando en una base de datos local del AP o con un servidor RADIUS externo. Un túnel VPN seguro acaba en un AP.
- Otra posibilidad es el uso de un servidor VPN central. El servidor VPN puede ser un dispositivo de Hardware o un ordenador en el que haya instalada una aplicación de software VPN. En la red LAN el túnel VPN va desde los clientes pasando por el AP hasta el servidor VPN . Si existen ya servidores VPN para accesos RAS (Servicio de Acceso Remoto) ya pueden ser usados en las redes LAN inalámbricas.

WPA (Acceso Wi-Fi Protegido)
Debido a los numerosos puntos débiles de las redes LAN inalámbricas, la Wi-Fi Alliance [3], trabajando en colaboración con la IEEE, dieron a conocer en octubre 2002 las especificaciones WPA, presentándolas como el software de seguridad que sustituiría al WEP [4].
La WPA es una especificación de implementaciones de seguridad basadas en estándares, que deben ser empleadas para los sistemas LAN inalámbricos. Esta medida tiene como objetivo suplir los déficit de seguridad del WEP. La mayoría de los WPA anteriores son compatibles con el estándar IEEE 802.11i, que se aprobó a finales del 2003.
En la especificación WPA se trató de sobre todo de que se pueda seguir utilizando el hardware ya disponible. Mediante actualizaciones de Software/Firmware para los AP y los

adaptadores de red inalámbricos se posibilita que estos puedan seguir utilizándose. Además se da la posibilidad de remplazar en el acto las encriptaciones WEP inseguras por otras sin dependencia del fabricante. La implementación más barata es apta tanto para empresarios como para redes particulares.
Para conseguir esta meta es necesario instalar dos mejoras esenciales de seguridad. Estas implementaciones son una codificación de datos mejorada y una autentificación de usuarios. Ambos aspectos no estaban contemplados en la protección WEP.

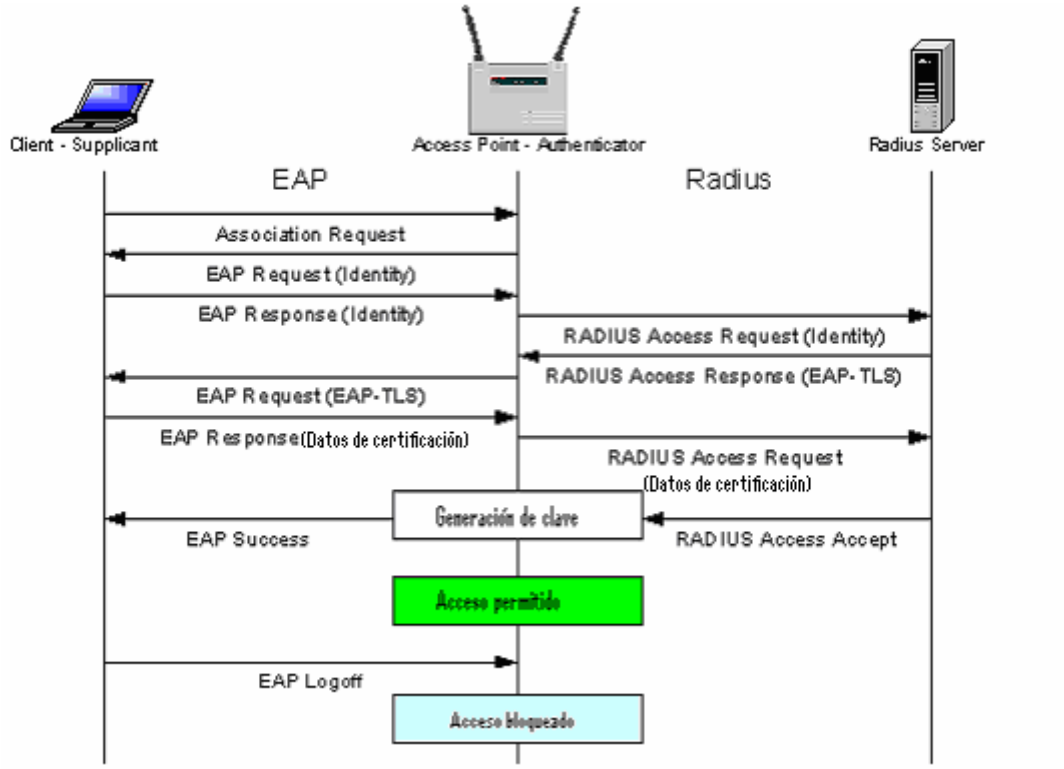
Mayor protección de datos con TKIP
Para una mejor codificación de datos el estándar WPA utiliza TKIP (Protocolo de integridad de clave temporal), con el que se reparan todos los puntos débiles de WEP en el área de la codificación de datos. El TKIP, posibilita esta mejora insertando un mecanismo per-packet-key. Es decir, que para calcular la clave se intercala una función HASH, que usa una clave distinta para cada paquete. Además en el TKIP hay incorporado un controlador de integridad de los datos mejorado, conocido como MIC (Código de integridad del mensaje) o como Michael. El MIC se utiliza para evitar la manipulación de los datos. El transmisor calcula el MIC a partir del MAC Header (direcciones del remitente y del destinatario), de la prioridad, y de los datos. El MIC se envía y el destinatario lo verifica tras descodificarlo. Los paquetes con un MIC falso son rechazados. Así se emiten ataques activos, posibles con las implementaciones WEP originarias y además se podrá instalar software.
Además hay integrados mecanismos de re-keying. Y un vector de inicialización ampliado (48 bits en lugar de 24). Con estas mejoras se eliminan todos los puntos débiles del WEP.

Mejor autentificación del usuario a través del estándar 802.1x y del EAP
En una red local deberían poder trabajar sólo aquellos usuarios que tengan la autorización para hacerlo. Dado a la exposición ilimitada de las ondas de radio (sin tener en cuenta el alcance limitado) y a la existencia del único método de autentificación que existía hasta el momento, por medio de la dirección MAC, hacían muy difícil controlar el acceso. WEP apenas contiene un identificador de usuario y al insertar el estándar 802.1x y el EAP (Protocolo de autentificación extensible) se resolvería el problema.
El estándar IEEE 802.1x [6] retoma este problema y posibilita la autentificación del usuario en el punto de acceso. El IEEE 802.1x fue concebido en un principio para las redes LAN basadas en Ethernet, para poder controlar el acceso directamente en el puerto de acceso, pero ahora, ha sido reforzado y también se emplea en las redes LAN inalámbricas. Al insertar el estándar 802.1x la autentificación de usuario se llevará a cabo directamente en el área de acceso a la red. Los derechos y programas propios de cada usuario no le serán asignados, es decir no tendrán acceso a ellos, hasta que se haya hecho una autentificación satisfactoria.
Los puntos básicos de este estándar son:

- el EAP (Protocolo de autentificación extensible), hace posible la comunicación entre clientes y servidores de autentificación (ej. RADIUS) a través de diversos posibilidades de autentificación.
- el propio estándar 802.1x para el acceso a redes basadas en puertos.

Funcionamiento de 802.1x:
El sistema está formado por tres componentes primarios [6]:

- el cliente (Supplicant), que se quiere autentificar, para conseguir el acceso a la red.
- el AP (Authenticator), que se encarga de de habilitar el puerto tras autenticar el cliente por medio del servidor de autenticación.
- EL servidor de autenticación (Authenticaton Server), que incluye los datos del usuario y comprueba si el cliente está autorizado para acceder a la red.



La figura muestra un esquema del proceso.
El cliente envía una petición al AP para acceder a la red. Éste intercambia de información con el servidor central de autenticación y desconecta el puerto, es decir, impide el acceso.
El núcleo del autenticador 802.1x forma el Protocolo de autenticación extensible (EAP). Este protocolo define la comunicación entre el llamado Supplicant (solicitante- portátil) y el Authenticator (AP) y respalda los diferentes métodos de autenticación. Dependiendo del método de autenticación se comprobará la identidad del usuario por medio del nombre de usuario, contraseña, certificados, etc... La petición de acceso pasa por el AP, que a su vez la envía al servidor de autenticación. Casi siempre se trata de un servidor RADIUS. En el servidor RADIUS se comprobará entonces, si la autentificación fue satisfactoria y si se puede dar acceso al puerto. El servidor RADIUS, sin embargo, no tiene que hacerse cargo de la autenticación, sino que puede reenviarla a otro servidor, (p.ej. LDAP, Active Directory, etc.) que tiene las ventajas de ser un administrador central de usuarios.
Se pueden utilizar como métodos autenticadores por ejemplo, MD5 (Message Digest 5), TLS (Transport Layer Security) o PEAP (Protected EAP).

WPA contiene las tecnologías, que ya estén disponibles y es la respuesta a las fuertes exigencias de los usuarios de las redes LAN inalámbricas, una solución de seguridad más fiable, que no depende del fabricante y de instalación inmediata, para los aparatos basados en tecnología Wi-Fi.
Algunas partes del estándar 802.11i tienen que ser retiradas para no tener que esperar la aprobación del mismo.

¿Qué elementos forman ya parte del WPA?

- IEEE 802.1x
- TKIP (Protocolo de integridad de clave temporal)

- Administración de claves
- Procesos de encriptación y autenticación

La certificación WPA comenzó en abril de 2003. La ratificación del estándar IEEE 802.11i se espera para comienzos del 2004, de modo que los primeros aparatos deberán estar disponibles a mediados del 2004. Según Wi-Fi Alliance a finales de 2004 se establecerá la especificación WPA v2 que incluye el equipamiento del estándar IEEE 802.11i completamente implementado.

IEEE 802.11i
[4]

El estándar IEEE 802.11i aún está en la fase de ratificación y cubrirá los puntos débiles del estándar 802.11 con numerosas mejoras y cambios.
"Marco del proyecto: *mejorar el Medium Access Control (MAC) 802.11 para mejorar los mecanismos de seguridad y autenticación" [7]*
Sin embargo los aparatos LAN inalámbricos usados hasta el momento deberían seguir siendo aprovechables (naturalmente con pérdidas en seguridad). Debido a las numerosas funciones nuevas, para los futuros estándares se necesitarán nuevos equipos. Los aspectos centrales en los futuros estándares de seguridad 802.11i son 802.1x, AES y EAP.
El estándar IEEE 802.11i debería cumplir los siguientes puntos:

- Inserción del TKIP compatible con el sistema actual, con las características antes mencionadas (Per-Pachet Keying, MIC, ampliación del IV, uso de los números de secuencia, etc.)
- Sustitución del algoritmo RC4 por el AES (Estándar de encriptación avanzado) para los nuevos equipos. El algoritmo RC4 usado en WEP se sustituye completamente en el estándar 802.11i por AES. Sin embargo, AES necesita nuevos equipos, ya que utiliza un mecanismo de encriptación diferente. Por razones de compatibilidad el estándar se basará también en RC4, pero esto sacrificará en cierto modo la seguridad.
- Autenticación a través de un puerto hecha con el estándar 802.1x, basada en EAP. 802.1x tiene un papel decisivo en el estándar 802.11i y posibilita la autenticación específica del usuario. Con el EAP también se podrán usar futuros mecanismos biométricos de autenticación.
- Generación de claves con un administrador de claves dinámico. El administrador de claves se efectuará con la inserción del estándar 802.1x y un servidor de autenticación.
- La autenticación recíproca del cliente y el AP para evitar ataques intencionados con puntos de acceso falsos.
- Grupos de claves jerárquicos.
- Administración dinámica de las opciones de autenticación y encriptación.

AES (Estándar de encriptación avanzada) [1]
En enero de 1997 el NIST (National Institute of Standards and Technology) inició el desarrollo de un estándar de encriptación avanzada. El estándar de encriptación dio lugar al FIPS (estándar de encriptado de datos federales) La especificación requería un proceso de encriptación simétrico basado en el cifrado en bloque con códigos de 128,192 y 256 bit. Del total de 15 participantes 5 llegaron a la última selección. Finalmentese eligió el algoritmo Rijndael.

El AES sustituirá en el estándar 802.11i al algoritmo RC4 utilizado hasta ahora. Con las implementaciones del AES en el estándar 802.11i se consiguen mejoras considerables en la encriptación. Actualmente AES es uno de los algoritmos de cifrado más potentes y de momento no se le ha encontrado ningún punto débil.
La repercusión negativa es que el software y firmware de los equipos han de ser actualizados para respaldar al algoritmo de encriptación. [8][9]

Como las ondas electromagnéticas se propagan más allá de los límites de los edificios, o de los solares, surgen otras posibilidades para que los atacantes penetren en la red. Si se implantaran las medidas de seguridad descritas más arriba, p.ej. Ipsec o perfeccionamiento de WEP, no se podría establecer ninguna diferencia en términos de confidencialidad e integridad, entre las redes inalámbricas y las convencionales. La mala fama se debe más bien a que la mayoría de los usuarios no emplean ninguna de las medidas descritas.

En cuanto a la disponibilidad de las redes, queda patente que las redes convencionales ofrecen más ventajas ya que un interferente, o un AP de alto puede suspender la red. Si la fiabilidad es un criterio importante para el usuario (ej. Dirección de maquinaria, etc.) no debería decantarse por las redes inalámbricas.

NOTAS

[1] Planet 3 Wireless (2002): CWNA Certified Wireless Network Administrator Official Study Guide (Exam PW0-100), Osborne/McGraw-Hill
[2] RFC 2661
[3] www.wi-fi.org
[4] Grasdal Martin, (2003): Defending your 802.11 Wireless Network, Syngress Publishing
[5] IEEE 802.11i Draft Standard, (2002): Draft Supplement to Standard for Telecommunications and Information Exchange between Systems – Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2002 D3, IEEE
[6] IEEE 802.1x Standard, (2001): Port-Based Network Access Control, 2001, IEEE
[7] www.ieee.org
[8] www.nist.gov, Report on the Development of the Advanced Encryption Standard AES) http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf
[9] www.nist.gov/aes, AES Homepage
[10] Fuhrberg Kai, 2000, Internet Sicherheit: Browser, Firewalls und Verschlüsselung
[11] Hein Mathias, 2002, TCP/IP 6ª edición.