Seguridad en WiFi (Resumen ejecutivo)

Por: Alejando Corletti Estrada.
Acorletti@hotmail.com

Madrid, mayo de 2005.

Este texo forma parte de una dupla que por razones de "Humanización", ha sido dividido en un Resumen Ejecutivo (más breve) y un informe técnico (casi inhumano). Basado en estas dos presentaciones se invita al lector a optar por el grado de detalle que desee. Los documentos son: Seguridad en WiFi (Resumen ejecutivo) - Seguridad en WiFi (Técnico).

Temario

DESARROLLO:

I. Presentación (Los estándares 802.11):

WiFi (Wireless Fidelity) es un nombre comercial desarrollado por un grupo de comercio industrial llamado WiFi Alliance (Inicalmente: 3Com – Aironet [hoy parte de CISCO] – Harris – Lucent – Nokia y Symbol technologies, hoy más de 150 miembros), el nombre "oficial" de esta alianza es **WECA** (Wireless Ethernet Compatibility Alliance) y son los primeros responsables de 802.11b.

WiFI describe los productos de WLAN basados en los estándares 802.11 y está pensado en forma más "Amigable" que la presentación eminentemente técnica que ofrece IEEE.

La web de esta alianza es
www.wi-fi.org
www.wifi-alliance.net

En esas web se puede también consultar el estado "on Line" de los productos que se encuentran certificados, el path es: http://www.wi-fi.org/OpenSection/Certified_Products.asp?TID=2

El estándar **802.11** de IEEE se publica en junio 1997, luego de seis años de proceso de creación. Propone velocidades de 1 y 2Mbps y un rudimentario sistema de cifrado (el **WEP**:Wired Equivalent Privacy), opera en 2,4 GHz con RF (Radio Frecuencia) e IR (Infra Rojo). Aunque WEP aún se sigue empleando, ha sido totalmente desacreditado como protocolos seguro.

En septiembre de 1999 salen a la luz el estándar **802.11b** que ofrece 11Mbps y el **802.11a** que ofrece 54 Mbps, si bien los productos de la primera aparecieron en el mercado mucho antes.

La familia 802.11, hoy se encuentra compuesta por los siguientes estándares:

- **802.11a:** (5,1-5,2 Ghz, 5,2-5,3 Ghz, 5,7-5,8 GHz), 54 Mbps. OFDM: Multiplexación por división de frecuencias ortogonal
- **802.11b:** (2,4-2,485 GHz), 11 Mbps.
- 802.11c: Define características de AP como Bridges.
- 802.11d: Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias).
- 802.11e: Calidad de servicio (QoS).
- 802.11f: Protocolo de conexión entre puntos de acceso (AP), protocolo IAPP: Inter Access Point Protocol.
- **802.11g**: (2,4-2,485 GHz), 36 o 54 Mbps. OFDM: Multiplexación por división de frecuencias ortogonal. Aprobado en 2003 para dar mayor velocidad con cierto grado de compatibilidad a equipamiento 802.11b.
- 802.11h: DFS: Dynamic Frequency Selection, habilita una cierta coexistencia con HiperLAN y regula también la potencia de difusión.
- **802.11i:** Seguridad (aprobada en Julio de 2004).
- 802.11j: Permitiría armonización entre IEEE (802.11), ETSI (HiperLAN2) y ARIB (HISWANa).
- 802.11m: Mantenimiento redes wireless.

Para acotar únicamente el tema de seguridad, se tratarán sólo 802.11a, b g y 802.11i.

Hoy en día se puede decir que existen tres estándares de WLAN:

- **HomeRF:** Es una inciativa lanzada por Promix, principalmente en EEUU y orientada exclusivamente al mercado residencial. Tiene sus bases en los estándares de teléfono digital inalámbrico mejorado (DECT)
- **BlueTooth:** Lo inició IBM, orientado al mercado comercial/ventas, y a la interconectividad de elementos de hardware. En realidad no compite con 802.11, pues tiene la intención de ser una estándar con alcance nominal de 1 a 3 metros y a su vez no supera los 1,5 Mbps
- **802.11:** Cubre todo el espectro empresarial.

Quizás el tema más importante a destacar es la posibilidad de expansión de 802.11. El incremento constante de mayores velocidades, hace que los 11 Mbps de 802.11b, estén quedando pequeños. La migración natural es hacia 802.11g, pues sigue manteniendo la frecuencia de 2,4GHz, por lo tanto durante cualquier trancisión en la que deban convivir, ambos estándares lo permiten. En cambio si se

comienzan a instalar dispositivos 802.11a, los mismos no permiten ningún tipo de compatibilidad con 802.11b, pues operan en la banda de 5 GHz.

Una iniciativa que se debe mencionar también es **HiperLAN** en sus versiones 1 y 2. Se trata de una verdadera analogía inalámbrica para ATM. Fue un competidor de 802.11 que opera en la frecuencia de 5 GHz y gozó del apoyo de compañías como Ericsson, Motorola, Nokia; Panasonic y Sony, se llegaron a crear regulaciones por parte de ETSI al respecto, pero no se logró imponer y hoy en día está prácticamente en desuso. En lo particular me hace acordar mucho a la batalle que hubo entre ATM y Ethernet (Fast ethernet, giga ethernet....).

II. Seguridad en WiFi:

Los tres aspectos fundamentales que se deben tener en cuenta al diferenciar una red WiFi de una cableada, son:

- Autenticación
- Control de acceso
- Confidencialidad

1. Autenticación y control de acceso:

Los métodos que se emplean son los siguientes:

a. SSID (Service Set Identifier): Contraseña (**WEP**: Wired equivalent Protocol).
b. Seguridad por restricción de direccionamiento MAC (Múmero de seis octetos que identifca univocamente a la tarjeta):
c. Contraseñas no estáticas:
    - Periódicas:
    - OTP (One Time Password): Contraseñas de un solo uso, conocidas como token flexibles.

d. **802.1x:** Este estándar no fue presentado para WiFi, sino para el acceso seguro PPP. Se trata del método más seguro actualmente.

    La arquitectura 802.1x está compuesta por tres partes:
    - **Solicitante:** Generalmente se trata del cliente WiFi
    - **Auenticador:** Suele ser el AP (Punto de acceso), que actúa como mero traspaso de datos y como bloqueo hasta que se autoriza su acceso (importante esto último).
    - **Servidor de autenticación:** Suele ser un Servidor RADIUS (Remote Authentication Dial In User Service) o Kerberos, que intercambiará el nombre y credencial de cada usuario. El almacenamiento de las mismas puede ser local o remoto en otro servidor de LDAP, de base de datos o directorio activo.

    Otra de las grandes ventajas de emplear 802.1x es que el servidor de autenticación, permite también generar claves de cifrado OTP muy robustas, tema en particular que ya lo posiciona como imprescindible en una red WiFi que se precie de segura.

e. **802.11i** (esto en realidad aplica también a confidencialidad): El Task Group de IEEE 802.11i se conformó en el año 2001 con la intención de analizar una arquitectura de seguridad más robusta y escalable, debido a la inminente demanda del mercado en este tema y en julio de 2004 aprobó este estándar. Por su parte la WiFi Alliance lo lanzó al mercado en septiembre de ese año.

   En forma resumida, este nuevo estándar, propone a 802.1x como protocolo de autenticación, pudiendo trabajar con su referencia **EAP** (Extensible Authentication Protocol: **RFC 2284**), este último proporciona una gran flexibilidad (sobre todo a los fabricantes) en la metodología de autenticación.

   Previo al estándar, varios fabrticantes ofrecieron métodos de autenticación:**LEAP, PEAP, EAP/TLS**, **EAP/TTLS.** Lo importante es el grado de flexibilidad que el estándar 802.11i ofrece hacia los mismos, pues soporta a la mayoría de ellos.

2. Cifrado:

a. **WEP:** Protocolo extremadamente débil y actualmente en desuso.

b. Las deficiencias de WEP, se están tratando de solucionar en la actividad de cifrado, a través del protocolo **TKIP** (Temporal Key Integrity Protocol). Esta propuesta aparece a finales de 2002 y propone tres mejoras importantes:
   - **Combinación de clave por paquete:** Generando trillones de claves diferentes, una para cada paquete.
   - **VI** (Vector de inicialización) de **48 bits**: Este tema era una de las mayores debilidades de WEP al emplear sólo 24 bits.
   - **MIC** (Message Integrity Check): Se plantea para evitar el conocido ataque inductivo o de hombre del medio. Y propone descartar todo mensaje que no sea validado.

c. Microsoft ofrece otra alternativa que inicialmente denominó **SSN** (Simple Security Network), el cual es una implementación de TKIP al estilo Microsoft. SSN lo adoptó 802.11i renombrándolo como **WPA** (WiFi Protected Access), en el año 2004 aparece **WPA2** que es la segunda generación del WPA . Este ya proporciona encriptación con un fuerte algoritmo llamado **AES** (Norma de Encriptación Avanzada) y está contemplado en IEEE 802.11i . En realidad 802.11i propone un "Mix" de funciones criptográficas cuyo eje central es AES, y lo bautiza como **CCMP**, su nombre completo proviene el "**Counter mode" (CTR**) que habilita la encriptación de datos y **el Cipher Block Chaining Message Authentication Code (CBC-MAC)** para proveer integridad, y de ahí su extraña sigla CCMP. La mayoría de los fabricantes están migrando hacia este algoritmo y se aprecia que será el estándar que se impondrá en el muy corto plazo.

3. VPNs: La última opción que se menciona aquí es la aplicación de VPNs. Esta alternativa no responde a ningún estándar de WiFi, pero se trata de llevar al wireless toda la experiencia y solidez que tiene hoy esta tecnología.. Existen muchos tipos de VPNs, que no se mencionarán aquí, por no ser parte de WiFi, pero sí se debe aclarar que es una opción muy válida y de hecho se está implementado cada vez con mayor frecuencia en las opciones de wireless.

III. Problemas concretos de Seguridad en WiFi:

a. **Puntos ocultos:** Este es un problema específico de las redes inalámbricas, pues suele ser muy común que los propios empleados de la empresa por cuestiones de comodidad, instalen sus propios puntos de acceso. Este tipo de instalaciones, si no se controlan, dejan huecos de seguridad enormes en la red. El peor de estos casos es la situación en la cual un intruso lo deja oculto y luego ingresa a la red desde cualquier ubicación cercana a la misma. La gran ventaja que queda de este problema es que es muy fácil su identificación siempre y cuando se propongan medidas de auditorías periódicas específicas para las infraestructuras WiFi de la empresa, dentro del plan o política de seguridad.
b. **Falsificación de AP** (Punto de Acceso)**:** Es muy simple colocar una AP que difunda sus SSID, para permitir a cualquiera que se conecte, si sobre el mismo se emplean técnicas de "Phishing", se puede inducir a creer que se está conectando a una red en concreto.
c. **Deficiencias en WEP**: Ya existen varias herramientas automáticas para descifrarlo.
d. **ICV independiente de la llave**: Se trata de un control de integridad débil, cuya explotación permite inyectar paquetes en la red.
e. **Tamaño de IV demasiado corto**: Como se mencionó, es el principal problema del protocolo WEP.
f. **Deficiencias en el método de autenticación:** Si no se configura adecuadamente una red WiFi posee débil método de autenticación, lo cual no permite el acceso, pero si hacerse presente en la misma.
g. **Debilidades en el algoritmo key Scheduling de RC4:** Este el el algoritmo de claves que emplea WEP, y con contraseñas débiles existen probabilidades de romperlo. Esto fue la sentencia definitiva para WEP.
h. **Debilidad en WPA:** Nuevamente existe un tema de seguridad con el empleo de claves débiles (esto lo soluciona la versión dos de WPA).

IV. Medidas de Seguridad en WiFi:

a. Emplear las **mismas herramientas que los intrusos**: realizar la misma actividad, pero para el "lado bueno".
b. **Mejorar la seguridad física**.
c. Cancelar puertos que no se emplean,
d. **Limitar el número de direcciones MAC** que pueden acceder. Esta actividad se realiza por medio de ACLs (Access List Control) en los AP.
e. **Satisfacer la demanda:** Si se están empleando AP no autorizados por parte de los empleados, es porque les resulta útil, por lo tanto, se pueden adoptar las medidas para que se implanten, pero de forma segura y controlada, de otra forma, seguirán apareciendo, pero de forma clandestina.
f. **Controle el área de transmisión:** Todos los puntos de acceso inalámbrico permiten ajustar el poder de la señal.
g. **Implemente la autenticación de usuario:** Mejore los puntos de acceso para usar las implementaciones de las normas WPA2 y 802.11i.
h. **Proteja la WLAN con la tecnología "VPN Ipsec" o tecnología "VPN clientless":** esta es la forma más segura de prestar servicios de autenticación de usuario e integridad y confidencialidad de la información en una WLAN.

i. **Active el mayor nivel de seguridad que soporta su hardware:** incluso si tiene un equipo de un modelo anterior que soporta únicamente WEP, asegúrese de activarlo. En lo posible, utilice por lo menos una WEP con un mínimo de encriptación de 128 bits.
j. **Instale firewalls personales y protección antivirus en todos los dispositivos móviles:** la Alianza WiFi recomienda imponer su uso continuo.
k. **Adquiera equipamiento que responda a los estándares** y certificado por "WiFi Alliance".

V. Conclusiones

Como se trató de explicar en el texto, una red WiFi en si misma no es segura o insegura. **Este valor lo dará la implementación de la misma.**

Evidentemente se está haciendo un gran esfuerzo, tanto en los organismos de estandarización como en los fabricantes (que en definitiva son los mismos actores) para ofrecer productos que se puedan configurar tan seguros como una red cableada. Sobre esta tarea no puede haber dudas, pues el factor determinante es **LA CONFIANZA** que generen estas redes al público en general (como sucede con el comercio electrónico), si la gente no CONFÍA, entonces estos productos no se venden, como el interés de los fabricantes es la venta, su principal preocupación es generar esta CONFIANZA por medio del esfuerzo en **garantizar** la seguridad de las mismas.

Lo que se puede afirmar al analizar el estándar **802.11i**, es que se están haciendo las cosas bien, pues tanto **802.1x**, como **AES (o CCMP)**, son dos mecanismos extremadamente sólidos y que actualmente se los puede catalogar como seguros en los tres aspectos fundamentales que hoy se ponen en dudas respecto a WiFi, es decir en autenticación, control de accesos y confidencialidad.

A lo largo de este texto se trató de describir brevemente la infraestructura WiFi, para avanzar luego en los tres aspectos más importantes (Autenticación, control de accesos y confidencialidad). Lo que se debe destacar es el **estándar 802.11i como algo importante en la seguridad WiFi** y que en definitiva **presenta una oferta SEGURA,** tanto (o más) que una red cableada, si se lo configura adecuadamente.

Las reflexiones finales son:

- Los **datos y la voz viajarán juntos** (ojo con esto que rompe muchas estructuras actuales), lo cual hará imprescindible metodologías inalámbricas por el concepto de movilidad.
- El **futuro se viene desde el aire** (WiFi y UMTS {que se trata en otro texto}).
- El factor **seguridad** debe ser una **preocupación de cada enlace**, y bien hecho (**802.11i**) puede ser tan seguro como antes. Por eso es importante **respetar** productos que apliquen **este estándar** (y no propietarios), y configurar sus parámetros correctamente.
- Si se implementas las medidas adecuadas en WiFi, es más simple ingresar a una empresa y conectar una portátil a la primera boca de red libre, que tomarse el trabajo de "escuchar", decodificar e intentar ingresar por aire.