Existen diversas maneras de poner a prueba la seguridad Wi-Fi de una red inalámbrica: una alternativa consiste en que el intruso intente conectarse a un access point de la red inalámbrica para luego ganar acceso a la red corporativa; la otra, consiste en “implantar” un access point pirata para atraer o los usuarios desprevenidos o muy curiosos a una red de hackers o red pirata.
Es preciso comprender que en las redes wireless la información se transmite por medio de ondas de radio frecuencia, las cuales están en el aire, y es imposible impedir que sea observada y/o capturado por cualquiera que se encuentre en un radio aproximado de 100 metros.

Problemática y Peligros de las Redes Wireless
Enumeramos algunos de los principales peligros que debemos tener en cuenta para mejorar la seguridad Wi-Fi.

* Cualquier otro usuario en un radio aproximado de 100 metros puede ser un “intruso potencial", bien con intención o sin ella.
* ¿Quién nos asegura que nos estamos conectando al servidor que deseamos? Como administradores de una red, ¿quién nos asegura que cada uno que intente conectarse a la misma es “de los nuestros”?

Debemos asegurarnos que, una vez establecida la conexión, ésta sea SEGURA o, lo que es lo mismo, ENCRIPTADA.
En las redes inalámbricas Wi-Fi existen 2 tramos por los que viajan los paquetes que llevan la información: un tramo inalámbrico (aéreo), que es el que va desde cada equipo Wi-Fi hasta el access point; y un tramo cableado, que es el que va desde el access point hasta el servidor de la organización.

Al no poder impedir de ninguna manera que la información que está en el aire sea vista por cualquiera, esta debe ser protegida por medio de protocolos de encriptación. En la actualidad

se utilizan WEP, WPA y WPA2.

En los comienzos (años 2000-2001), los productos de Wi-Fi incluían el protocolo de encriptación WEP (Wired Equivalent Privacy) basado en el algoritmo de codificación RC4, pero hace ya varios años los expertos comenzaron a advertir sus debilidades e Internet se inundó de aplicaciones, como Airsnort para crackearlo en una hora aproximadamente. Por ello, fue necesario buscar nuevas soluciones de seguridad para las redes Wi-Fi.

Esto originó el nuevo estándar 802.11i, el cual incluye 2 fases. La primer fase es temporal, y se vino aplicando el último par de años hasta que fueran diseñados y producidos nuevos access points y tarjetas Wi-Fi que soporten los cálculos requeridos por AES. En la fase temporal se utilizó el protocolo WPA (Wi-Fi Protected Access) basado en el TKIP. Desde ahora, todos los equipas serán nativos WPA2 (AES) y si no, no serán certificados.

"Al requerir WPA2 para todos los productos CERTIFICADOS Wi-Fi, estamos ayudando o que toda la gente esté segura de que la última generación en materia de seguridad está incluida, built in y lista para ser utilizada", dijo Frank Hanzlik, Director General de lo Wi-Fi Alliance.

En la página web de la Wi-Fi Alliance se pueden ver todos los productos certificados y los estándares que cada uno soporta. También se puede ver qué protocolos de autenticación EAP soportan y si son compatibles con el estándar 802.1 x de la IEEE. Según el comunicado de la Alianza, desde Septiembre de 2004 ya han certificado aproximadamente 600 productos que soportan WPA2, hasta ahora de manera opcional.