# CIFRADO EN REDES INALÁMBRICAS

Cifrado WEP, WPA y WPA2

24 DE NOVIEMBRE DE 2014

ADRIÁN CALVO ÉZARA

# Índice

# Introducción

Actualmente una de las formas más utilizadas para conectarse a Internet es por medio de una conexión WiFi, un sistema que ofrece al usuario importantes ventajas respecto a la conexión mediante cable, como por ejemplo movilidad, facilidad de instalación, amplia cobertura, etc. Pero este sistema tiene también inconvenientes, y uno de ellos hay que tenerlo muy en cuenta: la seguridad de nuestra red.

Entre los principales problemas que nos podemos encontrar con las redes WiFi está el robo del ancho de banda, una situación que se puede dar habitualmente si no se toman medidas. También tenemos que tener en cuenta que si disponemos de una conexión sin cifrar, la información que circula por esa red lo hará de forma pública, por lo que cualquier usuario que se encuentre en el espacio cubierto por la red podría capturar esa información, haciendo uso de unas simples aplicaciones.

Para resolver estos problemas de seguridad que presenta una red inalámbrica, tendremos que usar algún sistema de cifrado que requiera de algún tipo de credencial para poder navegar por esa red. Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11.

Los distintos sistemas que nos podemos encontrar en la actualidad los veremos a continuación.

# Cifrado WEP (Wired Equivalent Privacy)

El sistema de cifrado WEP fue el primero que apareció para solucionar los problemas generados por las redes abiertas. Se trata de un sistema de cifrado que funciona mediante la autenticación del usuario con contraseña. De esta forma el tráfico viaja cifrado, y aquel usuario que se encuentre escuchando el tráfico sólo leerá caracteres sin sentido alguno, a no ser que tenga la clave de cifrado.

## Objetivos

En la publicación de WEP se enunciaron una serie de objetivos que se pretendía que cumpliera:

- Ser razonablemente fuerte. Tiene una clave relativamente larga, y un vector de inicialización que va cambiando la clave efectiva usada en cada paquete.
- Tener la capacidad de que paquete se pueda encriptar y desencriptar por sí solo. Esto es imprescindible en una WLAN, ya que los paquetes perdidos representan un alto porcentaje. Supondría un gran problema que perder un paquete impidiera desencriptar los siguientes.
- Ser eficiente y poderse implementar en hardware o software.
- Ser exportable. Poder utilizarse en todo el mundo.
- Ser opcional.

## Modos de funcionamiento

El sistema de seguridad propuesto por el primer estándar tenía dos modos de operación posibles:

- Open Security, que en la práctica no representaba ninguna seguridad. Se corresponde con la autenticación, en la cual el dispositivo cliente envía un simple mensaje de solicitud de autenticación, al que el punto de acceso contesta con un mensaje de aprobación.

- Shared Key, que se basa en el conocimiento por parte de ambos extremos de una clave que debe permanecer secreta.

La seguridad WEP se puede descomponer en dos partes. En la primera se lleva a cabo la autenticación, y una vez completada con éxito, la segunda se encarga de la encriptación de los mensajes. Esta encriptación sirve también para continuar autenticando cada mensaje.

### Autenticación WEP

En este tipo de autenticación, existirá una clave secreta, que será empleada sobre un algoritmo para encriptar y desencriptar mensajes. De esta forma para ser capaz de enviar un mensaje hay que saber como encriptarlo y así estamos demostrando que somos un usuario autorizado. La autenticación se basa en la posesión de una clave.

### Encriptación WEP

El sistema de cifrado está basado en el algoritmo de cifrado RC4, utilizando para ello claves de 64 o de 128 bits. Cada clave consta de dos partes, una de ellas la tiene que configurar el usuario en cada uno de los puntos de acceso de la red, mientras que la otra se genera automáticamente y se denomina vector de inicialización, cuyo objetivo es obtener claves distintas para cada trama que se mueve en la red.

### Debilidades WEP

1. El propio algoritmo RC4 tiene alguna debilidad que se puede aprovechar para descifrar las claves aunque el principal fallo está en cómo se utiliza este algoritmo no en el propio RC4.
2. El estándar WEP permite que el vector de inicialización se pueda reutilizar (como promedio, cada cinco horas aproximadamente). Esta característica facilita mucho los ataques contra WEP, puesto que la repetición del VI garantiza que el atacante dispondrá de texto de cifrado repetido que analizar.
3. El estándar WEP no proporciona ninguna forma de cambiar las claves automáticamente. Como resultado, el cambio de clave de un punto de acceso (PA) y sus estaciones sólo se puede llevar a cabo manualmente; pero en la práctica, nadie cambia las claves, con lo que las redes LAN inalámbricas (WLAN) quedan expuestas a ataques pasivos en los que se recopila tráfico y se descifran las claves.
4. Las implementaciones WEP de los primeros escasos proveedores sólo ofrecían cifrado de 40 bits, una longitud de clave irrisoria. Los sistemas más modernos ofrecen cifrado WEP de 128 bits; la longitud de clave de 128 bits menos el VI de 24 bits proporciona en realidad una longitud de clave de 104 bits, que sería aceptable si no fuera por los otros inconvenientes.
5. No se garantiza la integridad de los mensajes. WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, por ejemplo, modificar algún número de la trama sin que el destino se percatara de ello.

## Cifrado WPA (Wi-Fi Protected Access)

Este sistema de cifrado surgió para solucionar los problemas de seguridad que ofrecía el sistema WEP. Para ello hace uso de TKIP, un protocolo para gestionar las claves dinámicas, que resuelve muchos de los problemas que tenía WEP tales como la longitud de la clave, el cambio

de la clave de estática a dinámica y la multidifusión. También incluye MIC (Message Integrity Code) o Michael, un código que verifica la integridad de los datos de las tramas.

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una clave precompartida, que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

### Modos de funcionamiento

- Enterprise Mode: (modo corporativo) con servidor. Éste es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- Home Mode: (modo personal) con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

### Debilidades WPA

Si se emplea WPA como mecanismo de seguridad los puntos de acceso únicamente aceptan autenticación y cifrado WPA, no permitiendo conectarse a usuarios sin WPA. Por otro lado, un usuario configurado para utilizar WPA no se conecta a puntos de acceso sin WPA. El problema que aún mantiene WPA es que se basa en el algoritmo de cifrado RC4, y como se ha comentado anteriormente ya se le han encontrado vulnerabilidad.

## Cifrado WPA2

WPA2 soluciona los problemas de vulnerabilidad detectados en la primera versión (WPA), e incorpora todas las características del estándar IEEE 802.11i.

Este sistema presenta dos cambios principales respecto a WPA:

- El reemplazo del algoritmo Michael por un código de autenticación conocido como el protocolo “Counter-Mode/CBC-Mac” que es considerado criptográficamente seguro.
- Reemplazo del algoritmo RC4 por el algoritmo AES, uno de los más seguros actualmente.

### Debilidades WPA2

Tiene el inconveniente de que no todos los routers permiten este tipo de cifrado, además de no ser compatible con el sistema WAP. Teóricamente, la difusión y multidifusión de claves representan otra vulnerabilidad. Todos los nodos de la red necesitan conocerlas, y un atacante que descubra una de las claves puede, al menos, espiar el intercambio de claves entre el punto de acceso y la estación de trabajo.

## Comparativa cifrados

**Tabla 1: Comparativa tecnologías de cifrado Wireless**

| Tecnología | Integridad | Cifrado | Autenticación | Protocolo |
|---|---|---|---|---|
| **WEP** | CRC-32 *Cyclic redundancy check* | RC4 (Mal implementado) | Sistema abierto o clave compartida | |
| **WPA** | MIC o Michael *Message authentication code* | RC4 | PSK (*Pre-shared key*) Radius | TKIP *Temporal Key Integrity Protocol* |
| **WPA2** | AES *Advanced Encryption Standard* | AES *Advanced Encryption Standard* | PSK (*Pre-shared key*) Radius | CCMP *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* |

## Bibliografía

http://www.saulo.net/pub/inv/SegWiFi-art.htm, consultado por última vez 23/11/2014.

http://www.acens.com/wp-content/images/whitepaper-redes-seguridad-acens-julio-2012.pdf, consultado por última vez 23/11/2014.

http://trajano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20redes%20Wifi%20Eduroam.pdf, consultado por última vez 23/11/2014.

http://www.microsoft.com/spain/technet/recursos/articulos/11110305.aspx, consultado por última vez 23/11/2014.

http://www.egov.ufsc.br/portal/sites/default/files/riesgos_de_las_redes_inalambricas.pdf, consultado por última vez 23/11/2014.