

Protocolos de seguridad en redes inalámbricas

Saulo Barajas
Doctorado en Tecnologías de las Comunicaciones
Universidad Carlos III de Madrid
E-mail: correo at saulo.net

Abstract. *Security is a critical issue in wireless networks because it's easy that an eavesdropper listen to the packets transmitted. The IEEE 802.11 standard includes Wired Equivalent Privacy (WEP) to secure link-layer communications. However, this method has been broken using several ways. This article explains the most important security flaws of WEP and proposes new alternatives to this protocol. The protocol developed to replace WEP will be IEEE 802.11i (WPA2). But before the ratification of this new standard, expected in June 2004, it is already available a specification from Wi-Fi called WPA, which is a subset of IEEE 802.11i technologies.*

1 Introducción a WEP, WPA y WPA2

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Conscientes de este problema, el IEEE [1] publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11 [2]. Pero WEP, desplegado en numerosas redes WLAN, ha sido roto de distintas formas, lo que lo ha convertido en una protección inservible.

Para solucionar sus deficiencias, el IEEE comenzó el desarrollo de una nueva norma de seguridad, conocida como 802.11i [3], que permitiera dotar de suficiente seguridad a las redes WLAN.

El problema de 802.11i está siendo su tardanza en ver la luz. Su aprobación se espera para junio de 2004. Algunas empresas en vistas de que WEP (de 1999) era insuficiente y de que no existían alternativas estandarizadas mejores, decidieron utilizar otro tipo de tecnologías como son las VPNs para asegurar los

extremos de la comunicación (por ejemplo, mediante IPSec). La idea de proteger los datos de usuarios remotos conectados desde Internet a la red corporativa se extendió, en algunos entornos, a las redes WLAN. De hecho, como hemos comentado antes, ambos canales de transmisión deben considerarse inseguros. Pero la tecnología VPN es quizás demasiado costosa en recursos para su implementación en redes WLAN.

No ajena a las necesidades de los usuarios, la asociación de empresas Wi-Fi [4] decidió lanzar un mecanismo de seguridad intermedio de transición hasta que estuviese disponible 802.11i, tomando aquellos aspectos que estaban suficientemente avanzados del desarrollo de la norma. El resultado, en 2003, fue WPA [5].

Este artículo analiza las características de los mecanismos de seguridad WEP, WPA y WPA2 (IEEE 802.11i). En el momento de escribir estas líneas, WPA2 todavía no ha visto la luz por lo que la documentación relacionada es todavía muy escasa.

2 WEP

2.1 Características y funcionamiento

WEP (*Wired Equivalent Privacy*, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11 [2]. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autenticación y control de acceso en redes WLAN [2, §6.1.2]. Estudiamos a continuación las principales características de WEP.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la

clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El algoritmo de encriptación utilizado es RC4 con claves (*seed*), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP es el siguiente:

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, *Integrity Check Value*).
2. Se concatena la clave secreta a continuación del IV formado el *seed*.
3. El PRNG (*Pseudo-Random Number Generator*) de RC4 genera una secuencia de caracteres pseudoaleatorios (*keystream*), a partir del *seed*, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (*frame body*) de la trama IEEE 802.11.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el *seed* y con ello podrá generar el *keystream*. Realizando el XOR entre los datos recibidos y el *keystream* se obtendrá el mensaje sin cifrar (datos y CRC-32). A continuación se comprobará que el CRC-32 es correcto.

2.2 Debilidad del vector de inicialización

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que el IV es la parte que varía de la clave (*seed*) para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

Sin embargo, el estándar 802.11 no especifica cómo manejar el IV. Según [2, §8.2.3] se indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello. Queda abierta a los fabricantes la cuestión de cómo variar el IV en sus productos. La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama. Y esto ocasiona que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Más aún si tenemos en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

Por otro lado, el número de IVs diferentes no es demasiado elevado ($2^{24}=16$ millones aprox.), por lo que terminarán repitiéndose en cuestión de minutos u horas [6]. El tiempo será menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se repitiese nunca, pero como vemos, esto es imposible en WEP. La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etc.) y de la carga de la red. Observemos que es trivial saber si dos tramas han sido cifradas con la misma clave, puesto que el IV se envía sin cifrar y la clave secreta es estática.

La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Bien es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

¿Qué podemos hacer una vez hemos capturado varias tramas con igual IV, es decir, con igual *keystream*? Necesitamos conocer el mensaje sin cifrar de una de ellas. Haciendo el XOR entre un mensaje sin cifrar y el mismo cifrado, nos dará el *keystream* para ese IV. Conociendo el *keystream* asociado a un IV, podremos descifrar todas las tramas que usen el mismo IV. El problema es entonces conocer un mensaje sin cifrar, aunque esto no es tan complicado, porque existen tráfico predecibles o bien, podemos provocarlos nosotros (mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc.) [6].

Con lo que hemos descrito no podemos deducir la clave secreta, aunque sí es posible generar una tabla

con los IVs de los que sabemos su *keystream*, la cual permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla [6].

Sin embargo, podemos llegar a más y deducir la clave secreta. Una nueva vulnerabilidad del protocolo WEP [7] permite deducir la clave total conociendo parte de la clave (justamente, el IV que es conocido). Para ello necesitamos recopilar suficientes IVs y sus *keystreams* asociados obtenidos por el procedimiento anterior.

2.3 Otras debilidades de WEP

WEP también adolece de otros problemas [6, 8] además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4.

Entre los objetivos de WEP, como comentamos más arriba, se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado [6] 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. En lugar del algoritmo de CRC se recomienda como ICV (*Integrity Check Value*) un algoritmo diseñado para tal fin como SHA1-HMAC [9].

El estándar IEEE 802.11 incluye un mecanismo de autenticación de las estaciones basado en un secreto compartido [2, §8.1]. Para ello se utiliza la misma contraseña de WEP en la forma que describimos a continuación. Una estación que quiere unirse a una red, solicita al punto de acceso autenticación. El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió.

El mecanismo anterior de *autenticación de secreto compartido* tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad). El estándar es consciente de esta debilidad y aconseja no utilizar el mismo IV para el resto de transmisiones. Sin embargo, tanto si las implementaciones repiten ese IV como sino, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización explicadas más arriba [8].

WEP no incluye autenticación de usuarios. Lo más que incluye es la autenticación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autenticación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. En este caso

tendríamos una *autenticación de sistema abierto* [2, §8.1], es decir, sin autenticación.

Entre la larga lista de problemas de seguridad de WEP se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (*replay*). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica. El estudio de N. Borisov, I. Goldberg y D. Wagner [6] explica razonadamente que ninguno de los objetivos planteados por WEP se cumplen.

2.4 Alternativas a WEP

Las vulnerabilidades explicadas de WEP son motivos más que suficientes para utilizar otros mecanismos de seguridad en redes WLAN.

Aunque no forma parte del estándar, los fabricantes de productos Wi-Fi decidieron ofrecer la posibilidad de utilizar claves del doble de longitud (de 64 bits a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como *WEP2*. Sin embargo, debemos observar que la longitud del vector de inicialización sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar el IV), por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits). Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera. WEP2 no resuelve los problemas de WEP [6].

Otra variante de WEP utilizada en algunas implementaciones es *WEP dinámico*. En este caso se busca incorporar mecanismos de distribución automática de claves y de autenticación de usuarios mediante 802.1x/EAP/RADIUS. Requiere un servidor de autenticación (RADIUS normalmente) funcionando en la red. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de una trama, este mecanismo sería suficiente para compensar las principales debilidades de WEP.

Sin embargo, la solución preferida por las empresas como alternativa a WEP ha sido la utilización de VPNs, de la misma manera que se haría si los usuarios estuviesen conectados remotamente a la oficina. La tecnología de VPNs está suficiente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperabilidad entre dispositivos de distintos fabricantes.

Los mecanismos diseñados específicamente para redes WLAN para ser los sucesores de WEP son WPA [5] y WPA2 (IEEE 802.11i) [3]. El primero es de 2003 y el segundo se espera para 2004. Se estudian a continuación.

3 WPA

WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicarán en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaban suficientemente maduras y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

3.1 Características de WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autenticación.

WPA incluye las siguientes tecnologías:

- **IEEE 802.1X.** Estándar del IEEE de 2001 [10] para proporcionar un control de acceso en redes basadas en puertos. El concepto de *puerto*, en un principio pensado para las ramas de un *switch*, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP [11] y un servidor AAA (*Authentication Authorization Accounting*) como puede ser RADIUS (*Remote Authentication Dial-In User Service*) [12]. Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráfico o descartar otros).

- **EAP.** EAP, definido en la RFC 2284 [11], es el *protocolo de autenticación extensible* para llevar a cabo las tareas de autenticación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (*Point-to-Point Protocol*) [13], aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (*EAP over LAN*) [10].
- **TKIP** (*Temporal Key Integrity Protocol*). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama [4].
- **MIC** (*Message Integrity Code*) o Michael. Código que verifica la integridad de los datos de las tramas [4].

3.2 Mejoras de WPA respecto a WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2^{48} combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autenticación, se sustituye el mecanismo de autenticación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

3.3 Modos de funcionamiento de WPA

WPA puede funcionar en dos modos:

- **Con servidor AAA, RADIUS normalmente.** Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autenticación, autorización y contabilidad.

- **Con clave inicial compartida (PSK).** Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, 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 autenticación, pero no para el cifrado de los datos.

4 WPA2 (IEEE 802.11i)

802.11i [3] es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Se espera que esté concluido todo el proceso de estandarización para mediados de 2004. Wi-Fi [4] está haciendo una implementación completa del estándar en la especificación WPA2.

Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

WPA2 incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), desarrollado por el NIS [14]. Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol*) en lugar de los códigos MIC.

Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

5 Conclusiones

La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad.

El sistema WEP, incluido en la norma IEEE 802.11 para proporcionar seguridad, tiene distintas debilidades que lo hacen no seguro, por lo que deben buscarse alternativas.

Tanto la especificación WPA como IEEE 802.11i solucionan todos los fallos conocidos de WEP y, en estos momentos, se consideran soluciones fiables.

La ventaja de WPA es que no requiere de actualizaciones de hardware en los equipos. Mientras no se descubran problemas de seguridad en WPA, esta implementación puede ser suficiente en los dispositivos para los próximos meses.

La apuesta de seguridad del IEEE para sustituir al desafortunado WEP, 802.11i, todavía está pendiente de ser estudiada en profundidad por investigadores debido a que sus especificaciones no son públicas.

Referencias

- [1] Institute of Electrical and Electronics Engineers: <http://www.ieee.org>
- [2] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE Std 802.11, 1999 Edition.
- [3] Grupo de trabajo de IEEE 802.11i: <http://grouper.ieee.org/groups/802/11/>
- [4] Wireless Fidelity Alliance: <http://www.wi-fi.org>
- [5] Wi-Fi Protected Access: http://www.wi-fi.org/opensection/protected_access.asp
- [6] N. Borisov, I. Goldberg, D. Wagner, "Intercepting mobile communications: The insecurity of 802.11", julio de 2001.
- [7] S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", agosto de 2001.
- [8] W. A. Arbaugh, N. Shankar, Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", 2001.
- [9] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-hashing for message authentication", febrero de 1997.
- [10] "Port-Based Network Access Control", IEEE Std 802.1X-2001, junio de 2001.
- [11] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, marzo de 1998.
- [12] C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, junio de 2000.
- [13] W. Simpson, "The Point-to-Point Protocol (PPP)", RFC 1661, julio de 1994.
- [14] Computer Security Resource Center, National Institute of Standards and Technology: <http://csrc.nist.gov>