Protocolo de seguridad Wep

Overview

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 publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11. 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, 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 finales 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.

No ajena a las necesidades de los usuarios, la asociación de empresas Wi-Fi 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.

Con este trabajo, se pretende ilustrar las características, funcionamiento, aplicaciones, fallas y alternativas del protocolo de seguridad WEP.

Definición

WEP (*Wired Equivalent Privacy*, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas. En ningún caso es compatible con IPSec.

Estándar

El estándar IEEE 802.11 proporciona mecanismos de seguridad mediante procesos de autenticación y cifrado. En el modo de red Ad Hoc o conjunto de servicios avanzados, la autenticación puede realizarse mediante un sistema abierto o mediante clave compartida. Una estación de red que reciba una solicitud puede conceder la autorización a cualquier estación, o sólo a aquellas que estén incluidas en una lista predefinida. En un sistema de clave compartida, sólo aquellas estaciones que posean una llave cifrada serán autenticadas.

El estándar 802.11 especifica una capacidad opcional de cifrado denominada WEP (Wireless Equivalent Privacy); su intención es la de establecer un nivel de seguridad similar al de las redes cableadas. WEP emplea el algoritmo RC4 de RSA Data Security, y es utilizado para cifrar las transmisiones realizadas a través del aire.

Aunque los sistemas WLAN pueden resistir las escuchas ilegales pasivas, la única forma efectiva de prevenir que alguien pueda comprometer los datos transmitidos consiste en utilizar mecanismos de cifrado. El propósito de WEP es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN (es decir, proporcionar autenticación). Este propósito secundario no está enunciado de manera explícita en el estándar 802.11, pero se considera una importante característica del algoritmo WEP.

WEP es un elemento crítico para garantizar la confidencialidad e integridad de los datos en los sistemas WLAN basados en el estándar 802.11, así como para proporcionar control de acceso mediante mecanismos de autenticación. Consecuentemente, la mayor parte de los productos WLAN compatibles con 802.11 soportan WEP como característica estándar opcional**.**

Cifrado:

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida. El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.

Para proteger el texto cifrado frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto en claro, lo que genera un *valor de comprobación de integridad* (ICV). Dicho valor de comprobación de integridad se concatena con el texto en claro. El valor de comprobación de integridad es, de hecho, una especie de huella digital del texto en claro. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización. El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto ó que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden.

Autenticación:

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que

controla el acceso a la WLAN y evita accesos no autorizados a la red. De los dos niveles, la autenticación mediante clave compartida es el modo seguro. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el *desafío (challenge)*. La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.
La autenticación mediante clave compartida funciona sólo si está habilitado el cifrado WEP. Si no está habilitado, el sistema revertirá de manera predeterminada al modo de sistema abierto (inseguro), permitiendo en la práctica que cualquier estación que esté situada dentro del rango de cobertura de un punto de acceso pueda conectarse a la red. Esto crea una ventana para que un intruso penetre en el sistema, después de lo cual podrá enviar, recibir, alterar o falsificar mensajes. Es bueno asegurarse de que WEP está habilitado siempre que se requiera un mecanismo de autenticación seguro. Incluso, aunque esté habilitada la autenticación mediante clave compartida, todas las estaciones inalámbricas de un sistema WLAN pueden tener la misma clave compartida, dependiendo de cómo se haya instalado el sistema. En tales redes, no es posible realizar una autenticación individualizada; todos los usuarios, incluyendo los no autorizados, que dispongan de la clave compartida podrán acceder a la red. Esta debilidad puede tener como resultado accesos no autorizados, especialmente si el sistema incluye un gran número de usuarios. Cuantos más usuarios haya, mayor será la probabilidad de que la clave compartida pueda caer en manos inadecuadas.

Características
Según el estándar, WEP debe proporcionar confidencialidad, autentificación y control de acceso en redes WLAN. 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.

Algoritmos
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
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.

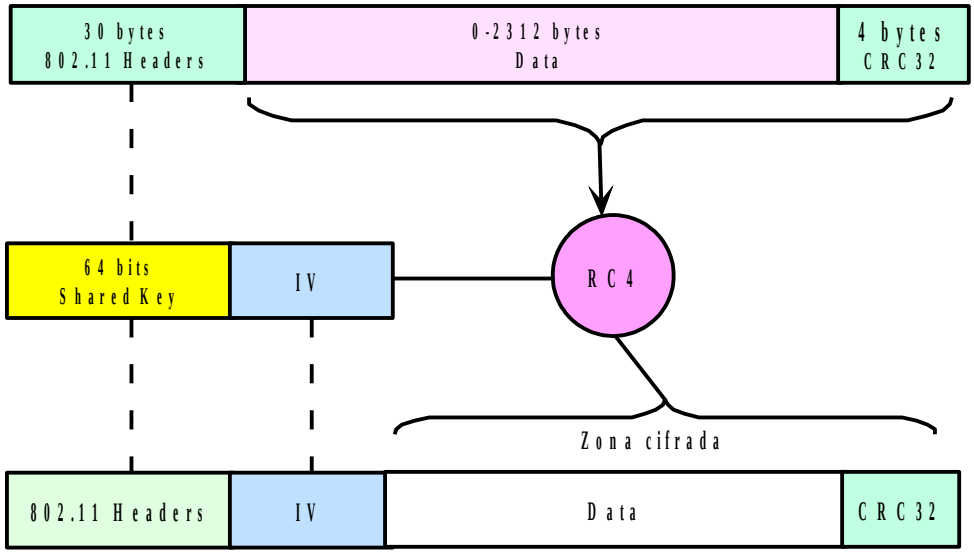

Figura 1. Algoritmo de Encriptación WEP

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), luego se comprueba que el CRC-32 es correcto.

Algoritmo de encriptación RC4

Es un algoritmo de Cifrador de flujo (no de bloques), creado en 1987 por Ronald Rivest (la R de RSA - Secreto Comercial de RSA Data Security). Fue publicado el 13 de Septiembre de 1994 usando remailers anónimos en un grupo de news: sci.crypt. Es usado por diversos programas comerciales como Netscape y Lotus Notes.

Funciona a partir de una clave de 1 a 256 bytes (8 a1024 bits), inicializando una tabla de estados. Esta tabla se usa para generar una lista de bytes pseudo-aleatorios, los cuales se combinan mediante la función XOR con el texto en claro; el resultado es el texto cifrado.

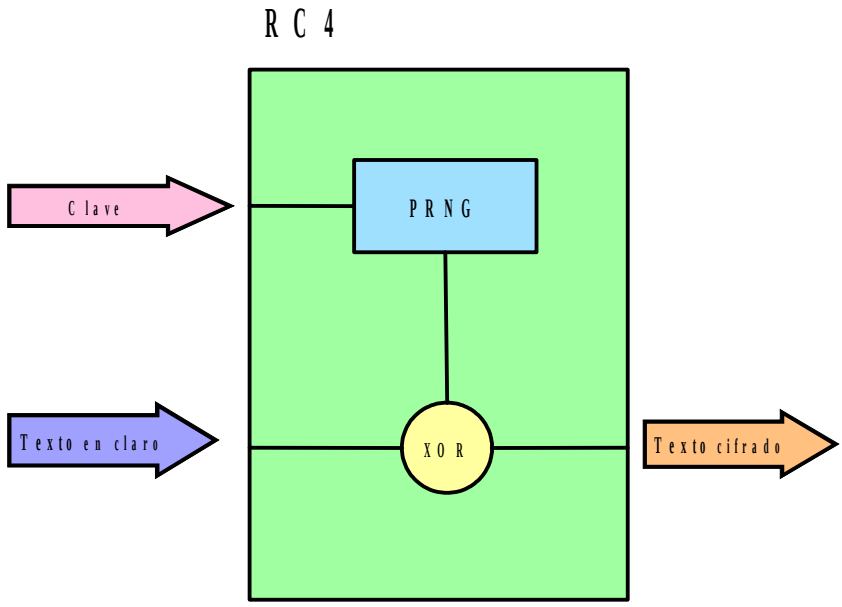

Figura 2. Cifrado RC4

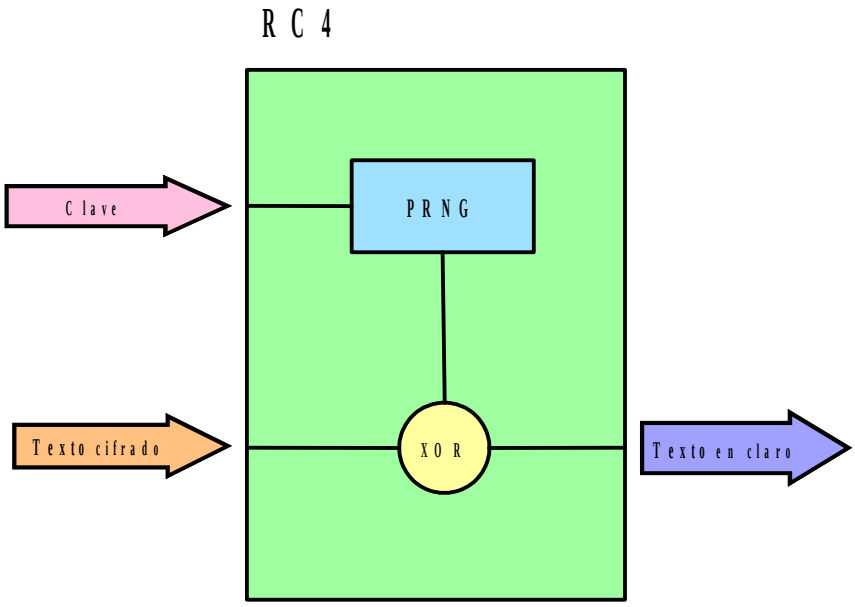

Figura 3. Descifrado RC4

Fallas de seguridad

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; 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. 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. 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.
La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse; 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.
Si se han capturado varias tramas con igual IV, es decir, con igual *keystream*, solo se necesita 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, se puede 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 tráficos predecibles o bien, se pueden provocar (mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc.).

Sniffing
Características sistemas Wireless:

- Es un sistema sin hilos y, por lo tanto, con una antena adecuada se puede interceptar todas las transmisiones de la celda (zona de un access point).
- Se emite de forma onmidirección por eso no se necesita afinar para capturar tráfico.
- Las estaciones utilizan franjas temporales asignadas por el Access Point para comunicarse, pero las antenas y tarjetas permiten escuchar en toda la banda.

Métodos de sniffing

- La antena es preferible que sea de Wireless LAN, pero pruebas con sistemas metálicos sencillos también han permitido sniffar a distancias cortas.
- Hay tarjetas y drivers preparados para monotorizar la red, son de alto coste.
- Con tarjetas de bajo coste sobre Linux se puede modificar para captar todo el tráfico.
- Un problema de algunas tarjetas de bajo coste es que deben pedir franja temporal y darse de alta en el AP y podrían ser detectadas. Se soluciona modificando Drivers.

Identificación de estaciones
Se identifican por la clave compartida con el AP. WEP no utiliza estados anteriores, esto permite reemplazar estaciones o realizar ataques de DoS. También es posible realizar ataques de repetición, volviendo a enviar paquetes capturados, que serán descifrados correctamente, si se descubre la clave, la estación intrusa tiene acceso a la LAN como si estuviera pinchando en las claves.
Ataques pasivos
Un ataque pasivo, es aquel donde se identifican secuencias pseudoaleatorias iguales. Ocurre por la debilidad de los algoritmos de streaming y del RC4. Fue descubierto por Fluher, Mantin y Shamir en agosto del 2001. Puede servir para realizar activos ya que con é se obtiene la clave.
Ataques activos
Entre los ataques activos se encuentra:

- *Repetición de paquetes*. Aprovechando que WEP no utiliza estados anteriores ni guarda estado.
- *Inyección o permutación de bits:* Utilizando el sistema de integridad débil.
- *Inyección de paquetes encriptados:* Si se conoce un texto y su encriptación, se puede encriptar un paquete sin conocer la clave.
- *Por 2 extremos*: Utilizando una máquina desde Internet se puede generar tráfico que luego sea cifrado por el AP hacia las estaciones wireless.

Identificación de secuencias pseudoaleatorias iguales

El criptograma es el resultado de realizar un XOR entre el generador pseudoaleatorio (RC4) y el texto, si se realiza un XOR de dos criptogramas con el mismo IV y clave (misma secuencia pseudoaleatoria) se obtiene el XOR de los 2 textos en claro.

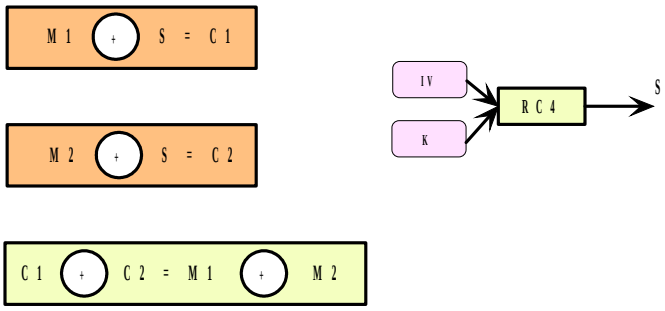

Figura 4. Id. Secuencias pseudoaleatorias iguales

Características de la identificación de secuencias pseudoaleatorias iguales:

- Aprovecha una debilidad de todos los algoritmos de streaming.
- Se deben utilizar métodos estadísticos, esto hace que no sea determinístico.
- Si se consiguen más mensajes con el mismo IV, la probabilidad de encontrar un texto en claro es mucho más alta.
- Cuando se encuentra uno todos los demás se pueden desencriptar.
- Es mejor el sistema que aprovecha la debilidad del RC4.

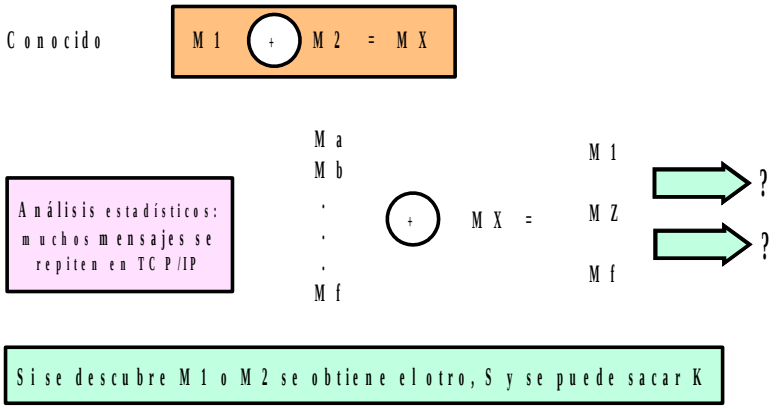

Figura 5. Id. Secuencias pseudoaleatorias iguales

Vulnerabilidad RC4

Fluhrer, Mantin y Shamir descubrieron en agosto del 2001 una debilidad del RC4. Se utiliza únicamente el primer byte generado por la secuencia pseudoaleatoria con el objetivo de obtener la clave de encriptación. También en agosto del 2001, Stubblefield, Ioannidis y Rubin implementaron un sistema práctico y barato para conseguir la clave con la vulnerabilidad del RC4. Consiguieron la clave en 2 tipos de experimentos con:

- Entre 5 y 6 millones de paquetes utilizando sólo la vulnerabilidad.
- Sobre 1 millón de paquetes combinando esta técnica con otras.

Los programas freeware Airsnort y WEPCrack utilizan esta técnica.

Cada paquete da información sobre un byte de la clave (pueden ser 40 o 102). Sólo un conjunto determinado de IV da información sobre una clave. Se deben buscar los paquetes con IV de un conjunto y a partir de éstos construir la clave de forma estadística. Para esto, se debe conocer el

texto en plano. En TCP/IP, se pueden utilizar los caracteres 0xAA que están en el inicio. En IPX se pueden utilizar los caracteres del inicio 0xFF o 0xE0.

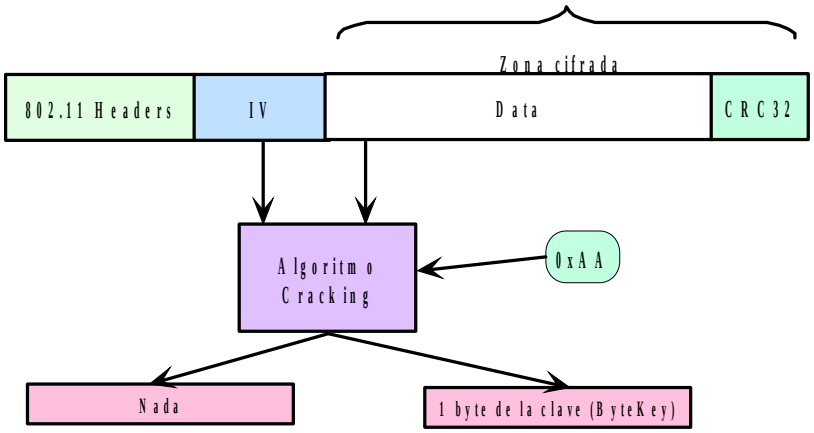

Figura 6. Vulnerabilidad RC4

Mejoras ataque vulnerabilidad RC4

- Para mejorar la eficiencia se pueden trabajar en paralelo varios tipos de IV.
- Un proceso analiza los IV (ByteKey + 3,0xFF, N) y otro proceso analiza otra estructura también vulnerable.
- Las claves se entran de forma manual, por lo tanto seguro que son vulnerables a los ataques de diccionario. Así cuando se tienen suficientes paquetes almacenados, se puede empezar la búsqueda de ByteKeys por las letras y números del alfabeto.
- Si se repiten dos valores iguales entre S[1], S[S[1]] y S[S[1] + S[S[1]]] entonces la probabilidad de encontrar la clave es mucho más alta. Si hay casos de estos almacenados se puede empezar trabajando con ellos.
- Realizar pruebas de fuerza bruta sobre los bytes que faltan utilizando el Checksum como comprobador de desencriptación correcta.
- Eliminar de la fuerza bruta los casos que se ha probado que un byte no forma parte de la clave. También eliminar de la fuerza los BytesKey de los que dispondremos de IV válidos. Los IV se pueden prever si su generación es deterministica (por ejemplo tipo contador).

Propuestas de soluciones sobre WEP actual

- Usar niveles de encriptación de niveles más altos, como Ipsec, etc...
- Colocar un Firewall entre los access points y la LAN.
- Usar VPNs.

Propuestas de soluciones sobre futuras versiones WEP

- Pasar la clave y el IV por una función Hash antes de introducirlos en el RC4. Se debe hacer en todas las estaciones.
- Cambiar el sistema de encriptación por un algoritmo simétrico más seguro, por ejemplo AES.
- Utilizar métodos de clave asimétrica para distribuir claves con el objetivo de:
  - Cambiar claves frecuentemente.
  - Utilizar claves aleatorias, no de diccionario.
  - Identificar de forma segura las estaciones.

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.
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 autentificación de usuarios mediante 802.1x/EAP/RADIUS. Requiere un servidor de autentificación (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 interoperatibilidad 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 finales de 2004.

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.
A pesar de la fortaleza potencial de WEP, incluido en la norma IEEE 802.11 para proporcionar seguridad, para proteger la confidencialidad e integridad de los datos, tiene una serie de limitaciones que solo se pueden evitar mediante una adecuada gestión. El primer problema surge en la utilización del vector de inicialización, el cual está incluido en la parte no cifrada del mensaje, para que el receptor conozca qué valor de IV (Vector de Inicialización) a utilizar a la hora de generar el flujo de clave para el descifrado. El estándar 802.11 recomienda, pero no exige, que el valor del IV se cambie después de cada transmisión. Si el valor del IV no se cambia de manera regular, sino que se utiliza para subsiguientes mensajes, alguien que esté realizando una escucha puede ser capaz de cripto-analizar el flujo de clave generado por el valor de IV y la clave secreta, y descifrar así los mensajes que utilicen dicho valor; lo que se vuelve aun más critico si se configura todos los terminales con las mismas claves.
El problema de la reutilización de valores de IV conduce, potencialmente, a otro problema; en concreto, una vez que un atacante conoce la secuencia de clave para un mensaje cifrado, basándose en los valores de IV utilizados, puede usar dicha información para generar una señal cifrada e insertarla en la red (usurpación y suplantación). El proceso consiste en crear un nuevo mensaje, calcular el calor CRC-32 y modificar el mensaje cifrado original para cambiar el texto en claro por el nuevo mensaje. El atacante puede entonces transmitir el mensaje a un punto de acceso o estación inalámbrica, que lo aceptará como mensaje válido. Cambiar el valor de IV después de cada mensaje es una forma simple de evitar tanto este problema como el problema descrito previamente.
La distribución de claves constituye otro problema. La mayor parte de las redes WLAN comparte una misma clave entre todas las estaciones y puntos de acceso de la red. Resulta poco probable que una clave compartida entre muchos usuarios permanezca secreta indefinidamente. Algunos administradores de red abordan este problema configurando las estaciones inalámbricas con la clave secreta ellos mismos, en lugar de permitir que los usuarios finales realicen esta tarea. Ésta es una solución imperfecta, porque la clave compartida continúa estando almacenada en las computadoras de los usuarios, donde es vulnerable. Además, si queda comprometida la clave en una única estación, todas las otras estaciones del sistema deberán ser reconfiguradas con una

clave nueva. La mejor solución entonces consiste en asignar una clave unívoca a cada estación y efectuar cambios de clave frecuentes.

Aunque el cifrado WEP está diseñado para ser computacionalmente eficiente, puede reducir el ancho de banda utilizable. De acuerdo con algunos informes, un cifrado de 40 bits reduce el ancho de banda en 1Mbps, mientras que el cifrado de 128 bits reduce el ancho de banda en una cantidad comprendida entre 1 y 2Mbps. Este grado de reducción es relativamente pequeño (sobre todo para los estándares 802.11a y g), pero los usuarios de 802.11 y 802.11b pueden llegar a percibirlo, especialmente si la señal se transmite utilizando FHSS (Frequency Hopping Spread Spectrum), que transmite las señales a un máximo de solo 3Mbps. En muchos casos, el impacto concreto dependerá del producto que se esté utilizando y del número de usuarios que haya en la red.

Concluimos en definitiva, que el protocolo WEP, es un leve intento por tratar de generar una privacidad y seguridad de los datos que se transmiten de manera inalámbrica, establecida por el IEEE en el 802.11; y como idea principal, la seguridad es directamente proporcional a la eficiencia y políticas que adopte el administrador de la red; lastimosamente, la carga administrativa y de gestión que se debe asumir al emplear este protocolo, es exagerada; por consiguiente es de notar, que el protocolo WEP, no debe ser la única herramienta y/o política para asegurar la confidencialidad, integridad y demás características de seguridad; se deben emplear un ramillete de alternativas complementarias, como el uso de VPNs (Redes Privadas Virtuales), o cualquier otro método como la encripción o implementar IPsec, etc. Además hay que destacar que el tener muy buenas políticas de seguridad en la red inalámbrica, trae la consecuencia que muy probablemente, se perderá el rendimiento y eficiencia en la velocidad de transmisión en la carga útil en la red, y es por esto, que en un diseño de red, es crucial determinar qué tipo de información y qué tipo de usuarios son los que dispondrían de servicio inalámbrico; y si es tan urgente mantener estrictos controles de seguridad, o si es relevante dejar que la información confidencial pueda ser transmitida por 802.11.

Palabras claves: seguridad, redes inalámbricas, wep, wlan, wi-fi, Wireless Equivalent Privacy, autenticación, encriptación, RC4, *sniffing*.

Bibliografía

[1] Institute of Electrical and Electronics Engineers. (Online). 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. (Online). http://grouper.ieee.org/groups/802/11/
[4] Saulo Barajas. Protocolos de seguridad en redes inalámbricas. (Online). http://www.saulo.net/pub/inv/SegWiFi-art.htm
[5] KDE. El cifrado WEP no es muy seguro en realidad (Online). http://www.kde.og
[6] Cabrera, Víctor A. Revista RED. (Online). http://www.red.com.mx/scripts/redArticulo.php3?idNumero=70&articuloID=7483
[7] VIRUSPROT.COM. (Online). De nuevo: las redes wireless no son seguras. http://www.virusprot.com/Nt240821.html
[8] Maximiliano Eschoyez. Seguridad en 802.11. (Online). http://lcd.efn.unc.edu.ar/frames/archivos/wep.pdf
[9] René GILLER. Wired Equivalent Privacy. (Online). http://lasecwww.epfl.ch/securityprotocols/wep/WEP.pdf
[10] Alapont, Vicent. Seguridad en redes inalámbricas. (Online). http://documentos.shellsec.net/otros/SeguridadWireless.pdf
[11] Varea, Felipe. Seguridad Informática en WLAN's. (Online). http://www.monografias.com/trabajos14/segur-wlan/segur-wlan.shtml
[12] . doc.: IEEE 802.11-00/362. (Online).
[13] Soumendra Nanda, Dartmouth Collage. (Online). http://www.dartmouth.edu
[14] Netmotion. Using NetMotion Mobility with WEP. (Online). www.netmotionwireless.com
[15] Cisco. Configuring Wired Equivalent Privacy (WEP). (Online). http:// www.cisco.com
[16] Tim Newsham. Cracking WEP Keys. Applying known techniques to WEP Keys. (Online). @Stake.

Javier Emilio Sierra,
Ingeniero Electrónico
javiersierrac@yahoo.es
Leonardo Betancur Agudelo,
Ingeniero Electrónico
leonardobetancuragudelo@yahoo.es
Marcela Maya Gómez,
Ingeniera Electricista
mmaya@upb.edu.co