Seguridad en Wi-Fi

Alberto Los Santos Aransay, *albertolsa@gmail.com*

Abstract— En el mundo multimedia actual una de las prioridades es lograr dotar de total ubicuidad a los servicios, para ello es necesario disponer de comunicaciones cada vez más avanzadas. Una de las características más importantes de las tecnologías de comunicaciones es la seguridad, principalmente cuando hablamos de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red, sin embargo, una red inalámbrica desplegada en una oficina podría ser accesible por un tercero sin ni siquiera estar ubicado en las dependencias de la empresa. Las redes inalámbricas necesitan métodos para cifrar los datos, autenticar a los usuarios, etc. En general, necesitan seguridad, aquí revisaremos cuáles son los principales mecanismos diseñados para Wi-Fi (IEEE 802.11).

***Index Terms*— 802.11i, Communication system security, WEP, Wi-Fi, WPA, WPA2**

I. Introducción

COMO hemos dicho, el canal de las redes inalámbricas, si no se realiza ninguna acción, es por sí sólo inseguro. La seguridad en la red no afecta de igual manera a todos los servicios desplegados sobre redes inalámbricas. No tiene los mismos requisitos un servicio que ofrece anuncios publicitarios en una red, en la cuál no importa que los usuarios capturen la información, y la repliquen con otro contenido, que un servicio de tráfico. Imaginemos que se dispone de un servicio de propagación de mensajes de seguridad vial a causa de accidentes, retenciones, cortes en las carreteras debido a condiciones climáticas, etc. Un usuario malicioso podría introducir información errónea provocando, por ejemplo, la detención de los vehículos debido a un supuesto accidente, o retardar el envío de esta información provocando un accidente mayor. De ahí que sea tan importante ofrecer la seguridad requerida en cada caso.

Junto a estos ejemplos, existen otras muchas técnicas así como tipos de ataques que un usuario malicioso puede realizar para perjudicar a los nodos de la red. En [1] se muestra una relación de las distintas amenazas que existen:

- Escucha de la información o análisis del tráfico.
- Inyección de mensajes.
- Eliminación de mensajes e intercepción.
- Enmascaramiento y AP malicioso: Las direcciones MAC se transmiten en los mensajes, y la mayoría de adaptadores pueden suplantar otros nodos.
- Secuestro de sesión (*Session Hijacking*).
- MitM (*Man-in-the-Middle*): Este ataque es distinto al de intercepción de mensajes, ya que el nodo malicioso debe participar en toda la comunicación, rompiendo el enlace entre los nodos reales si ya está establecido.
- Denegación de servicio: Los sistemas inalámbricos son muy vulnerables a los ataques DoS, pudiendo desbaratar la conexión entre los nodos legítimos.

Podemos establecer una serie de requisitos que deberían ser cumplidos por cualquier sistema de seguridad que quiera ser eficaz en este tipo de redes. Así, debemos disponer de autenticación para asegurar la legitimidad de los mensajes transmitidos a lo largo de la red, consistencia de los datos para confirmar que éstos no han sido alterados por ningún usuario malicioso, disponibilidad evitando que un usuario malicioso inhabilite la red utilizando inhibidores de frecuencia, no repudio y privacidad, posibilitando identificar a los nodos cuando sea necesario, pero a su vez que esta información sea confidencial.

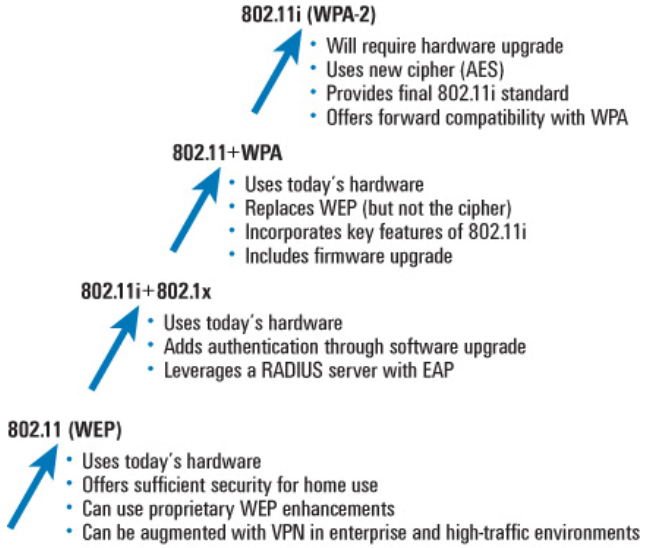

Fig. 1. Evolución de la seguridad en Wi-Fi. [2]

Conscientes de estos problemas y requisitos relativos con la seguridad sobre la norma 802.11 [3] de comunicaciones inalámbricas, el IEEE publicó un mecanismo opcional, denominado WEP. Como veremos, WEP 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 [4], que permitiera dotar de suficiente seguridad a las redes WLAN. Hasta la estandarización de 802.11i en 2004, surgieron otras medidas intermedias para complementar a WEP y sucederla. En este artículo analizaremos las características de los mecanismos de seguridad WEP, WPA y 802.11i (WPA2), sus debilidades, y trabajos complementarios para proteger las comunicaciones.

II. WEP (*WIRED EQUIVALENT PRIVACY*)

A. Descripción

WEP (*Wired Equivalent Privacy*) fue el sistema de cifrado incluido inicialmente en el estándar IEEE 802.11. Los objetivos de WEP son proporcionar confidencialidad, autenticación y control de acceso en redes WLAN [5]. El algoritmo de encriptación utilizado es RC4 con claves (*seed*), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits fijos correspondientes al vector de inicialización más 40 bits de la clave secreta. Estos 40 bits se deben distribuir manualmente, quedando almacenados en las estaciones.

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 misma. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. La clave secreta ya sabemos que es conocida; 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. Al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación en WEP es el siguiente [6]:

1) Se calcula un CRC (*Cyclic Redundancy Code*) 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 formando 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, obteniendo 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.

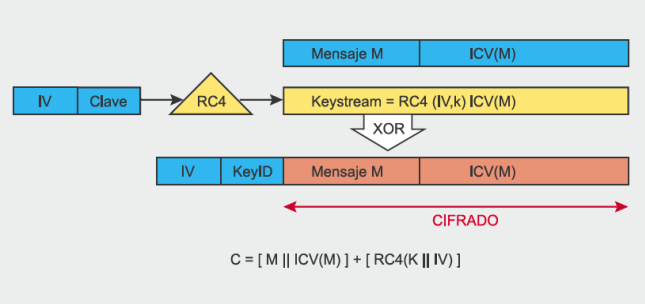

Fig. 2. Algoritmo de cifrado WEP [8]

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 debe comprobar que el CRC-32 es correcto.

B. Debilidades del algoritmo

Principalmente, la implementación del vector de inicialización (IV) en el algoritmo WEP ocasiona varios problemas de seguridad. El IV es la parte que varía de la clave para impedir que un posible atacante recopile suficiente información cifrada, sin embargo, el estándar 802.11 no especifica cómo manejar el IV, ya que indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello. Así, 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, ocasionando que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente.

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 [7], dependiendo de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etc.) y de la carga de la red.

WEP también adolece de otros problemas [7, 9] además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4. WEP incluye un CRC-32 que viaja cifrado para garantizar la integridad de los mensajes. 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. En lugar del algoritmo de CRC se recomienda como ICV (*Integrity Check Value*) un algoritmo diseñado para tal fin como SHA1-HMAC [10].

El estándar IEEE 802.11 incluye un mecanismo de autenticación de las estaciones basado en un secreto compartido. Así, 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. Este mecanismo 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 si no, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización ya explicadas [9].

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.

C. *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), conocido generalmente como *WEP2*. Sin embargo, 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 uso no varían, las debilidades del IV son las mismas y WEP2 no resuelve los problemas de WEP.

WEP+ [11] es una alternativa propietaria de la empresa Lucent Technologies, basada en la eliminación de los IV "débiles", pero no es integrada por muchos fabricantes.

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 el uso 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 y tiene como inconveniente la falta de interoperabilidad entre dispositivos de distintos fabricantes.

III. WPA (*Wi-Fi Protected Access)*

A. *Descripción y características*

WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi [16] a la seguridad que demandan los usuarios y que WEP no podía proporcionar. Debido a la tardanza en la publicación de la norma IEEE 802.11i (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 WPA.

WPA es, por tanto, un subconjunto del IEEE 802.11i [1]. Sus principales características 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 el protocolo TKIP [27] (*Temporal Key Integrity Protocol*), encargado de generar las claves para cada trama y asegurar la confidencialidad de los datos. Sigue utilizando RC4 para la encriptación de la información, pero incluye una función de mezclado de claves y un espacio extendido de IVs (para construir claves no correladas).

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 evitar duplicados. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*).

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.

WPA introduce el algoritmo *Michael*, un código para verificar la integridad de las tramas (MIC, *Message Integrity Code*) ligero. También provee dos mecanismos de autenticación. En el primero, los nodos son autenticados a través de una clave inicial compartida PSK (*Pre-Shared Key)*, este modo está orientado para usuarios domésticos o pequeñas redes. 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. La otra opción es el uso de IEEE 802.1X y el protocolo EAP (*Extensible Authentication Protocol*), que ofrecen mayor seguridad y generan una clave común como parte del proceso de autenticación.

IEEE 802.1X es un estándar para proporcionar un control de acceso en redes basadas en puertos. Se puede aplicar a las conexiones de un punto de acceso con las estaciones, así las estaciones tratarán de conectarse a un puerto del punto de acceso, manteniéndolo bloqueado hasta que el usuario se autentique. Con este fin se utiliza el protocolo EAP 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 (como priorizar ciertos tráficos o descartar otros).

Por otra parte, EAP (definido en la RFC 2284 [12]) 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*) [14].

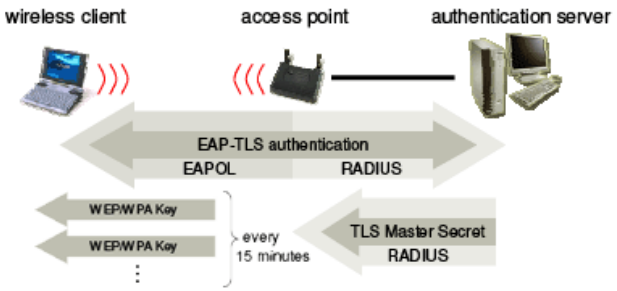

Fig. 3. Autenticación 802.1X usando EAP [31]

B. *Debilidades*

TKIP debería bastar para resolver todas las vulnerabilidades conocidas en WEP. Realmente mejora la seguridad en todos los aspectos, pero WPA desde sus orígenes también tiene debilidades. La función de mezcla de TKIP ofrece mayor seguridad que el correspondiente algoritmo en WEP, pero no es tan sólido como se pensaba, ya que es posible encontrar la clave MIC otorgada, además la seguridad completa puede ser rota durante la duración de una clave temporal (TK) dadas dos claves con el mismo IV32. Esto no significa que TKIP sea inseguro, pero ciertamente algunas partes son débiles.

Por otra parte, el algoritmo Michael está diseñado para dar sólo 20 bits de seguridad, minimizando la reducción en el rendimiento, por lo que un atacante puede lograr falsificar uno de cada 2^{19} paquetes. Existen medidas para limitar el ratio de estas falsificaciones, pero pueden dar lugar a ataques DoS.

Además, la autenticación 802.1X puede ser vulnerable a ataques de secuestro de *Session Hijacking* y *Man-in-the-Middle*. Estos ataques se evitan mediante el uso de autenticación mutua y fuerte encriptación, pero demuestran algunas de las posibles deficiencias.

En el siguiente capítulo veremos algunas debilidades de WPA2, que pueden ser comunes a WPA.

IV. WPA2 (IEEE 802.11i)

A. *Descripción*

802.11i [15] es el estándar del IEEE para proporcionar seguridad en redes WLAN. Concluida su estandarización a mediados de 2004, Wi-Fi hizo una implementación completa del estándar en la especificación WPA2.

WPA2, al igual que WPA, soporta el protocolo 802.1x para la autenticación [17] (por ej. en ámbitos empresariales) y la autenticación mediante clave compartida (PSK) (por ej. para los entornos SOHO, *Small Office and Home Office*, y ámbitos domésticos).

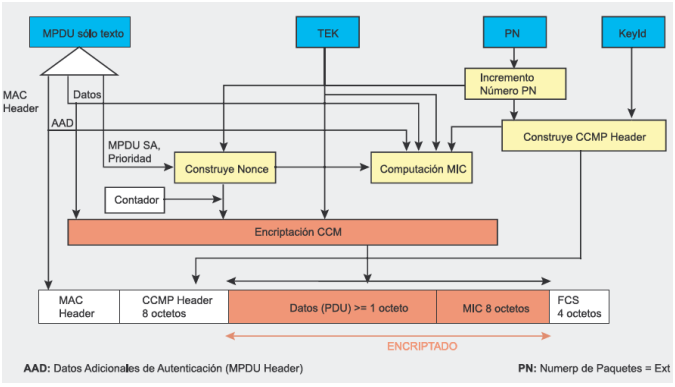

Fig. 4. Encriptación CCMP

WPA y WPA2 difieren poco conceptualmente, distinguiéndose principalmente en el algoritmo de cifrado que emplean. Mientras WPA se basa en el uso del algoritmo TKIP, que está basado en RC4 al igual que WEP, WPA2 utiliza CCMP [28] (*Counter-mode/CBC-MAC Protocol*) basado en AES (*Advanced Encrytion System*), más potente que TKIP. La segunda diferencia notable se encuentra en el algoritmo utilizado para controlar la integridad del mensaje. Mientras WPA usa una versión menos elaborada para la generación del código MIC (*Message Integrity Code*), o código *"Michael"*, WPA2 implementa una versión mejorada de MIC.

La nueva arquitectura para las redes wireless se llama *Robust Security Network* (RSN). Además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica. Una RSN sólo aceptará máquinas con capacidades RSN, pero IEEE 802.11i también define una red transicional de seguridad, *Transitional Security Network* (TSN), arquitectura en la que pueden participar sistemas RSN y WEP, permitiendo a los usuarios actualizar su equipo en el futuro. Si el proceso de autenticación o asociación entre estaciones utiliza *4-Way handshake* (proceso de negociación del estándar), la asociación recibe el nombre de RSNA (*Robust Security Network Association*).

El establecimiento de un contexto seguro de comunicación consta de cuatro fases:

- Acuerdo sobre la política de seguridad.
- Autenticación 802.1X.
- Derivación y distribución de las claves.
- Confidencialidad e integridad de los datos RSNA.

La información sobre la política de seguridad detalla los métodos de autenticación soportados (802.1X, PSK), protocolos de seguridad para el tráfico unicast (CCMP, TKIP etc.), la suit criptográfica basada en pares, protocolos de seguridad para el tráfico multicast (CCMP, TKIP etc.), suit criptográfica de grupo, soporte para la pre-autenticación, que permite a los usuarios pre-autenticarse antes de cambiar de punto de acceso en la misma red para un funcionamiento sin retrasos, etc.

La segunda fase es la autenticación 802.1X basada en EAP y en el método específico de autenticación decidido: EAP/TLS con certificados de cliente y servidor (requiriendo una infraestructura de claves públicas), EAP/TTLS o PEAP (*Protected Extensible Authentication Protocol*) para autenticación híbrida (con certificados sólo requeridos para servidores), etc.

La seguridad de la conexión se basa en gran medida en las claves secretas. En RSN, cada clave tiene una vida determinada y la seguridad global se garantiza utilizando un conjunto de varias claves organizadas según una jerarquía. Este entramado de claves muestra la complejidad del diseño del estándar. La generación y el intercambio de claves es la meta de la tercera fase.

En la cuarta fase se usan todas las claves generadas anteriormente en los protocolos que soportan la confidencialidad e integridad de datos RSNA: TKIP, CCMP y WRAP (*Wireless Robust Authentication Protocol*).

B. *Debilidades*

Aunque se han descubierto algunas pequeñas debilidades en WPA/WPA2 desde su lanzamiento, ninguna de ellas es peligrosa si se siguen unas mínimas recomendaciones de seguridad.

La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA/WPA2. La PSK proporciona una alternativa a la generación de 802.1X PMK (*Pairwise Master Key*) usando un servidor de autenticación.

Otra debilidad WPA es la posibilidad de negación del servicio durante el *4-Way Handshake* [30], ya que el primer mensaje del proceso no está autenticado, y cada cliente tiene que guardar cada primer mensaje hasta que reciban un tercer mensaje válido (firmado), dejando al cliente potencialmente vulnerable ante el agotamiento de memoria. Haciendo un *spoofing* del primer mensaje enviado por el punto de acceso, un atacante podría realizar un ataque DoS sobre el cliente si es posible que existan varias sesiones simultáneas.

El código de integridad de mensajes *Michael* tiene también debilidades conocidas que provienen de su propio diseño (forzado por el grupo de trabajo de 802.11i). La seguridad de Michael se basa en que la comunicación esté encriptada. Aunque los MICs criptográficos están generalmente diseñados para resistir a este tipo de ataques de texto conocidos (donde el atacante tiene un mensaje de texto y su MIC), *Michael* es vulnerable a estos ataques, porque es invertible. Si se le da un sólo mensaje y su valor MIC, se puede descubrir la clave secreta de MIC, así que mantener el secreto del valor de MIC es crítico.

La debilidad final conocida es la posibilidad teórica de un ataque contra el *Temporal Key Hash* de WPA, que implica una complejidad de ataque reducida bajo ciertas circunstancias (conocimiento de varias claves RC4).

WPA/WPA2 se ven sometidas a vulnerabilidades que afectan a otros mecanismos estándar de 802.11i, como son los ataques con *spoofing* de mensajes 802.1X (*EAPoL Logoff*, *EAPoL Start*, *EAP Failure* etc.), descubiertos en [29] y posibles gracias a una falta de autenticación. Por último, es importante destacar que el uso del protocolo WPA/WPA2 no tiene protección alguna frente a ataques sobre las tecnologías en que se basan, como puede ser la intercepción de frecuencias de radio, Negación del Servicio a través de violaciones de 802.11, de-autenticación, de-asociación, etc.

V. Extensiones de Seguridad

Para extender la seguridad en las comunicaciones, existen muy diversas posibilidades y estudios. Algunas son básicas y ya apenas mejoran la seguridad, mientras que otras son arquitecturas completas que combinan distintas tecnologías y elementos en base a cada escenario.

Algunos fabricantes de equipos ofertaron la opción de definir una lista de direcciones MAC no autorizadas, de esta forma se permitía extender ligeramente la seguridad, aunque pronto pasó a no ser útil, ya que las estaciones podían esnifar tráfico, obtener una MAC válida y usarla como propia [1].

Otro mecanismo básico, llamado *Closed System Authentication*, se basa en la ocultación del ESSID. De nuevo, no es muy útil, ya que el ESSID puede ser obtenido de forma sencilla a través de la trama *Probe Request/Response* o *(Re)Assotiation Request* de un usuario ya conectado.

Desde la capa física también se pueden aportar aproximaciones para proteger la comunicación, por ejemplo seleccionando antenas adecuadas y posiciones concretas se puede reducir la pérdida de señal, y mejorar la seguridad evitando posibles *frequency jammings*. Aparte, se pueden implementar *firewalls* RF, pero requiere modificaciones importantes en la capa PHY de 802.11.

Otra propuesta pretende mejorar 802.11i ante ataques DoS por inundación de peticiones de asociación, realizando antes el proceso de autenticación que el de asociación. En [18] se ofrece una versión basada en la acción indicada.

En diversos estudios se trabaja en acoplar distintas tecnologías para ofrecer *frameworks* de seguridad. Así, para controlar el acceso a la red y la autenticación, [19] propone una arquitectura adaptando 802.11i para soportar servicios de AAA (*Authentication, Authorization* y *Accounting*) utilizando EAP_TLS (*Transport Layer Security*) y EAP_Kerberos en escenarios con soporte de comunicaciones *Ad-hoc*.

En [21] proponen una arquitectura de seguridad para redes WLAN basada en el estándar 802.11i. En este tipo de estudios, se pretende lograr una combinación óptima de tecnologías en las distintas capas para proteger el sistema en cuestión. Además, en cada caso se tiene que tener en cuenta los recursos disponibles, ya que ciertas redes como las WSN (*Wireless Sensor Networks*) o las VANETs (*Vehicular Ad-hoc Networks*) tienen ciertas características restrictivas.

Centrándonos en escenarios concretos, en este caso vehiculares, en [22, 23, 24, 25] se muestran esquemas o arquitecturas de seguridad adaptados a redes de vehículos. Dichos esquemas mantienen una parte común que es la del uso de los mecanismos para garantizar la integridad, autenticidad, y cifrado de los mensajes así como garantizar la privacidad del usuario a través del uso de pseudónimos, pares de claves anónimas o de firmas ciegas (*blind signatures*) manteniendo la posibilidad de poder obtener la identidad del usuario en caso de exigencia de responsabilidades.

Por último, en [20], se muestra un estudio sobre AAA para redes de vehículos. Destacan el uso de Curvas elípticas criptográficas en lugar de las basadas en polinomios. Estas herramientas garantizan con un menor tamaño de clave la misma garantía que una de mayor tamaño en mecanismos como RSA de claves asimétricas. También hacen uso de pseudónimos para garantizar la privacidad de los usuarios.

VI. 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 solucionaban todos los fallos conocidos de WEP y, en su momento, se consideraron soluciones fiables, pero como hemos visto existen ya numerosos ataques que logran su propósito.

Lógicamente, a la hora de elegir cómo proteger las redes, es mejor decantarse por WPA2 debido a que la fortaleza de cifrado de AES es netamente superior a la de TKIP. Sin embargo, si no se cuenta con el hardware que soporte esta tecnología es perfectamente válido el uso de WPA pues la principal vulnerabilidad de WPA y WPA2 no se encuentra en el algoritmo de cifrado sino en la fortaleza de la clave utilizada.

Aún así, con el aumento de la capacidad de procesamiento de las nuevas máquinas y el interés de ciertas personas en romper la seguridad y/o estudiar el límite de los sistemas actuales, en el futuro se descubrirán más debilidades en los mecanismos de 802.11i, lo que hará que haya que trabajar sobre él para ofrecer características complementarias, y/o nuevos estándares que lo sustituyan.

Fig. 5. La seguridad en las comunicaciones, un reto [32]

REFERENCIAS

[1] C. He y J. C. Mitchell, "*Security Analysis and Improvements for IEEE 802.11i*" he 12th Annual Network and Distributed System *Security* Symposium (NDSS'05), pages 90-110. Feb. 2005.

[2] Imagen extraída de: http://www.dell.com/content/topics/global.aspx/power/en/ps3q03_lowerywireless?c=us&l=en&cs=555

[3] Grupo de trabajo de 802.11: http://www.ieee802.org/11/

[4] Estándar IEEE 802.11i-2004: http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[5] "*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*", ANSI/IEEE Std 802.11, 1999 Edition.

[6] S. Barajas, "*Protocolos de seguridad en redes inalámbricas*". Universidad Carlos III de Madrid.

[7] N. Borisov, I. Goldberg, D. Wagner, "*Intercepting mobile communications: The insecurity of 802.11*", julio de 2001.

[8] G. Lehembre, "S*eguridad Wi-Fi – WEP, WPA y WPA2*". Revista hakin9, enero de 2006.

[9] W. A. Arbaugh, N. Shankar, Y.C. Justin Wan, "*Your 802.11 Wireless Network has No Clothes*", 2001.

[10] H. Krawczyk, M. Bellare, R. Canetti, "*HMAC: Keyed-hashing for message authentication*", febrero de 1997.

[11] J. Revelo y E. Pazmiño, "*Análisis de WPA/WPA2 vs WEP*". Escuela Politécnica del Ejército. Febrero de 2008.

[12] L. Blunk, J. Vollbrecht, "*PPP Extensible Authentication Protocol (EAP)*", RFC 2284, marzo de 1998.

[13] W. Simpson, "*The Point-to-Point Protocol (PPP)*", RFC 1661, julio de 1994.

[14] "*Port-Based Network Access Control*", IEEE Std 802.1X-2001, junio de 2001.

[15] Grupo de trabajo de IEEE 802.11i: http://grouper.ieee.org/groups/802/11/

[16] Wireless Fidelity Alliance: http://www.wi-fi.org

[17] *Blog* "Un Informático en el lado del mal": http://elladodelmal.blogspot.com/2008/08/atacar-wpawpa2-psk-parte-i-de-iv.html

[18] D. B. Faria and D. R. Cheriton. "*DoS and authentication in wireless public access networks*". In Proceedings of the First ACM Workshop on Wireless Security (WiSe'02), Atlanta, Georgia, USA, September, 2002.

[19] H. Moustafa, G. Bourdon, Y. Gourhant, "*AAA in Vehicular Communication on Highways with Ad hoc Networking Support: A Proposed Architecture*", in Proceedings of 2nd ACM International Workshop on Vehicular Ad Hoc Networks (VANET-05), Cologne, Germany, Sept 2005, pp. 79-82.

[20] E. Coronado and S. Cherkaoui, *"An AAA Study for Service Provisioning in Vehicular Networks"*, in 32nd IEEE Conference on Local Computer Networks (2007).

[21] N. Wei, J. Zhou, Y. Xin, L. Li, "*A Security Architecture for IEEE 802.11 Wireless Networks in Large-Scale Multinational Corporations*". ITS Telecommunications Proceedings, 2006 6th International Conference. Junio de 2006.

[22] N.W. Wang, Y.M. Huang, W.M. Chen, "*A novel secure communication scheme in vehicular ad hoc networks*", Computer Communications (2008).

[23] S. Eichler, "*A Security Architecture Concept for Vehicular Networks Nodes*", in Proceedings of 6th International Conference on Information, Communications and Signal Processing (ICICS 2007), Singapore, Diciembre 2007.

[24] C. T. Li, M.S. Hwang, Y.P. Chu, "*A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks*", Computer Communications (2008).

[25] K. Plöbl y H. Federrath, "*A privacy aware and efficient security infrastructure for vehicular ad hoc networks*", Computer Standards & Interfaces (2008).

[26] G. Zuccardi y J. D. Gutiérrez, "*Seguridad Informática en 802.11*". Enero de 2006.

[27] Referencia a TKIP: http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

[28] RFC 3610, algoritmo de encriptación CCM: http://www.ietf.org/rfc/rfc3610.txt

[29] A. Mishra, W. A. Arbaugh, *"An Initial Security Analysis of the IEEE 802.1X Standard,"* CS-TR-4328, UMIACS-TR-2002-10, University of Maryland, College Park, MD, 2002.

[30] C. He, J. C. Mitchell, "*Analysis of the 802.11i 4-way handshake*". Proceedings of the 3rd ACM workshop on Wireless security. 2004.

[31] Imagen extraída de: http://www.usenix.org/events/sec04/tech/full_papers/balfanz/balfanz_html/eap-tls.gif

[32] Imagen extraída de: http://www.nbsp.es/images/2009/02/Candado.jpg