

Seguridad Informática en 802.11

Giovanni Zuccardi
Juan David Gutiérrez

Enero de 2006

Contenido

1. Introducción
2. WEP
3. Método Shared Key
4. 802.11i (WPA2)
5. IEEE 802.1X, EAP y RADIUS
6. Referencias
7. Bibliografía

1. Introducción

Dado el aumento en productividad y la creciente popularidad de las comunicaciones inalámbricas en general, y particularmente las de transmisión de datos de forma inalámbrica, es que nace idea de crear distintas soluciones con el fin de proporcionar un procedimiento a los asuntos de seguridad relacionados con estos, y arquitecturas del estándar IEEE 802. 11, buscando reducir la brecha en cuando a seguridad se refiere entre una red convencional y una inalámbrica. Como también, que se pueda diseñar una arquitectura sólida con un énfasis en la seguridad que permita acceso a la red en áreas donde tradicionalmente sería difícil instalar una red con cables.

2. WEP

WEP utiliza el algoritmo RC4 para la encriptación con llaves de 64 bits, aunque existe también la posibilidad de utilizar llaves de 128 bits. Veremos que en realidad son 40 y 104 bits, ya que los otros 24 van en el paquete como Vector de Inicialización (IV).

La llave de 40 ó 104 bits, se genera a partir de una clave (passphrase) estática de forma automática, aunque existe software que permite introducir esta llave manualmente.

A partir de la clave o passphrase se generan 4 llaves de 40 bits, sólo una de ellas se utilizará para la encriptación WEP.

Se hace una operación XOR con la cadena ASCII (*My Passphrase*) que queda transformada en una semilla de 32 bits que utilizará el generador de números pseudoaleatorios (PRNG) para generar 40 cadenas de 32 bits cada una.

Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave y se generan 4 llaves de 40 bits. De estas 4 llaves sólo se utilizará una para realizar la encriptación WEP.

El proceso de encriptación en conjunto se ve resumido en la siguiente grafica:

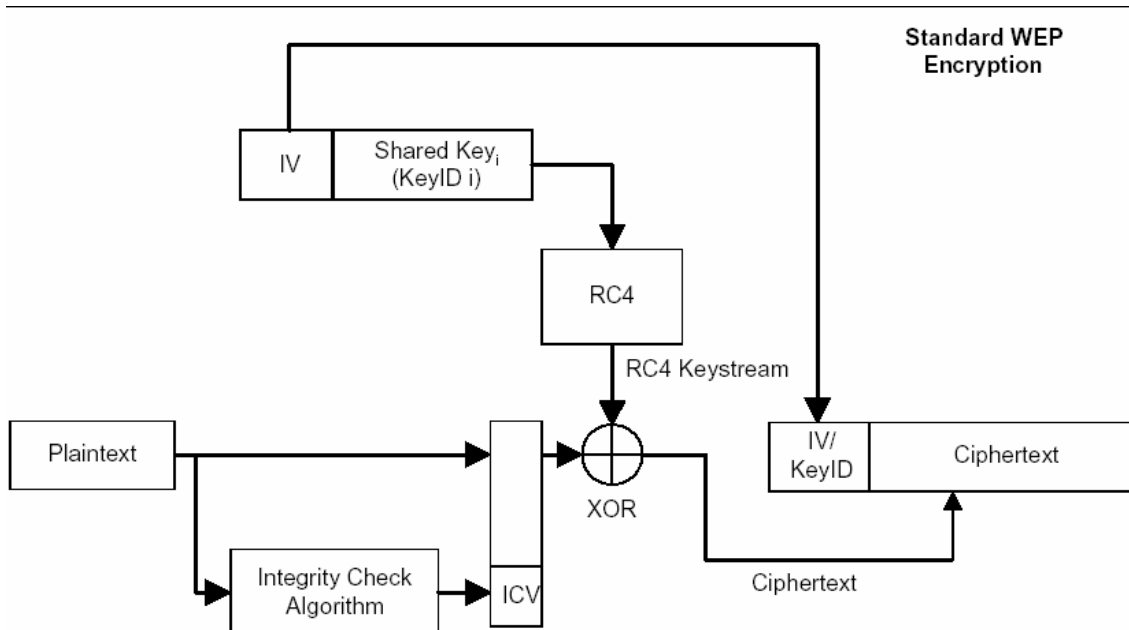


Figura 1: Proceso de encriptación WEP. [INSEG]

El proceso contrario es ilustrado en la siguiente grafica:

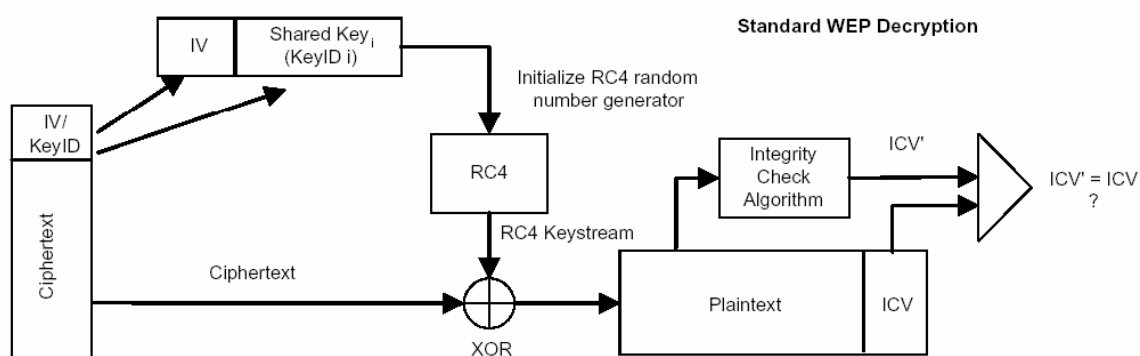


Figura 2: Proceso de desencriptación WEP. [INSEG]

Como hemos visto anteriormente, el campo ICV (Integrity Check Value) de una trama encriptada con WEP contiene un valor utilizado para verificar la integridad del mensaje. Esto provee un mecanismo de autenticación de mensajes a WEP, por lo tanto el receptor aceptará el mensaje si el ICV es válido. El ICV se genera simplemente haciendo un CRC (Cyclic Redundancy Check) de 32 bits, del payload de la trama. Este mecanismo tiene dos graves problemas:

- Los CRCs son independientes de la llave utilizada y del IV
- Los CRCs son lineales: $CRC(m \oplus k) = CRC(m) \oplus CRC(k)$

3. Método Shared Key

La estación que quiere autenticarse (cliente), envía una trama AUTHENTICATION REQUEST indicando que quiere utilizar una “clave compartida”. El destinatario (AP) contesta enviando una trama que contiene 128 octetos de texto (desafío) al cliente. El texto del desafío se genera utilizando el PRNG (generador de números pseudoaleatorios de WEP) con la clave compartida y un vector de inicialización (IV) aleatorio.

Una vez el cliente recibe la trama, copia el contenido del texto de desafío en el payload de una nueva trama, que encripta con WEP utilizando la clave compartida (*passphrase*) y añade un nuevo IV (elegido por el cliente). Una vez construida esta nueva trama encriptada, el cliente la envía al AP, y éste descrypta la trama recibida y comprueba que:

- El ICV (Integrity Check Value) sea válido (CRC de 32 bits).
- El texto de desafío concuerde con el enviado en el primer mensaje.

Si la comprobación es correcta, se produce la autenticación del cliente con el AP y entonces se vuelve a repetir el proceso pero esta vez el primero que manda la trama con el AUTHENTICATION REQUEST es el AP. De esta manera se asegura una autenticación mutua.

4. 802.11i (WPA2)

El estándar 802.11i fue adoptado y recibió el nombre comercial WPA2 por parte de la alianza Wi-Fi. El estándar IEEE 802.11i introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos.

El establecimiento de un contexto seguro de comunicación consta de cuatro fases (ver Figura 4):

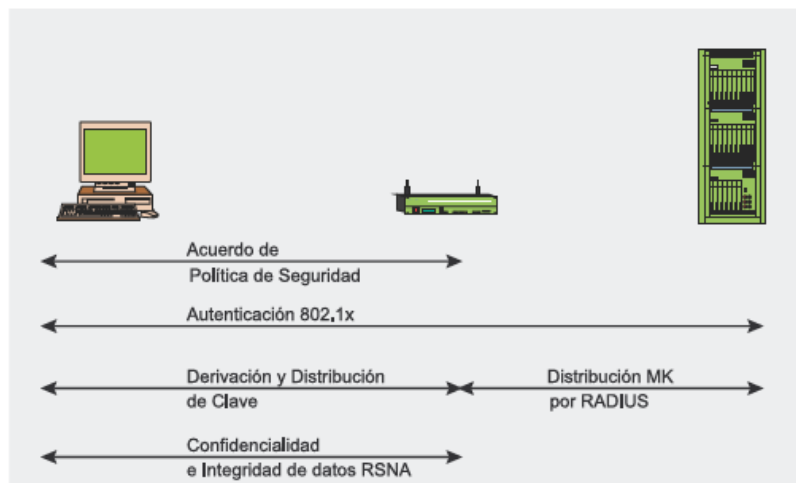


Figura 4: Fases Operacionales 802.11i. [SEGWF]

La primera fase requiere que los participantes estén de acuerdo sobre la política de seguridad a utilizar. Sigue a esto una autenticación abierta estándar (igual que en las redes TSN, donde la autenticación siempre tiene éxito). La respuesta del cliente se incluye en el mensaje de *Association Request* validado por una *Association Response* del punto de acceso. La información sobre la política de seguridad se envía en el campo RSN IE (*Information Element*) y detalla:

- Los métodos de autenticación soportados (802.1X, Pre-Shared Key (PSK)).
- Protocolos de seguridad para el tráfico unicast (CCMP, TKIP etc.) – la suite criptográfica basada en pares.
- Protocolos de seguridad para el tráfico multicast (CCMP, TKIP etc.) – suite 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.



Figura 5: Fase 1. [SEGWF]

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 para autenticación híbrida (con certificados sólo requeridos para servidores), etc. La autenticación 802.1X se inicia cuando el punto de acceso pide datos de identidad del cliente, y la respuesta del cliente incluye el método de autenticación preferido. Se intercambian entonces mensajes apropiados entre el cliente y el servidor de autenticación para generar una clave maestra común (MK). Al final del proceso, se envía desde el servidor de autenticación al punto de acceso un mensaje *Radius Accept*, que contiene la MK y un mensaje final *EAP Success* para el cliente.

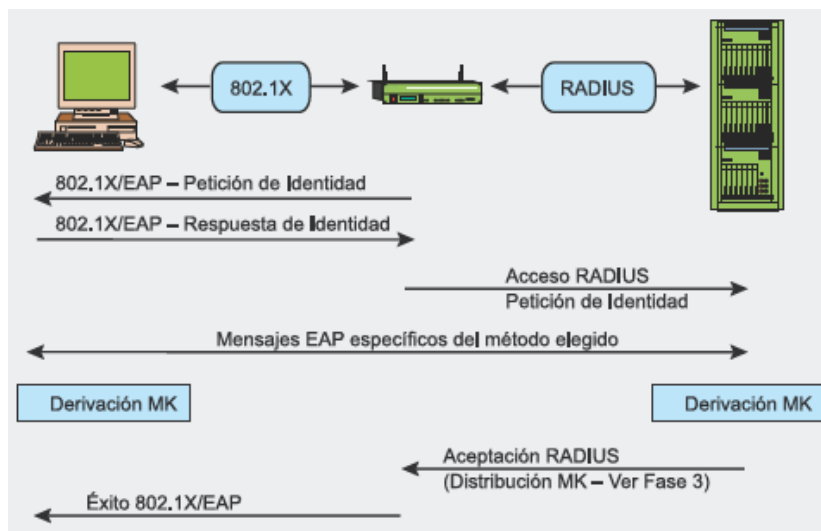


Figura 6: Fase 2. [SEGWF]

La tercera fase trata la distribución y jerarquía de las claves. 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. Cuando se establece un contexto de seguridad tras la autenticación exitosa, se crean claves temporales de sesión y se actualizan regularmente hasta que se cierra el contexto de seguridad. La generación y el

intercambio de claves es la meta de la tercera fase. Durante la derivación de la clave, se producen dos handshakes:

- *4-Way Handshake* para la derivación de la PTK (*Pairwise Transient Key*) y GTK (*Group Transient Key*),
- *Group Key Handshake* para la renovación de GTK.

La derivación de la clave PMK (*Pairwise Master Key*) depende del método de autenticación:

- Si se usa una PSK (*Pre-Shared Key*), $PMK = PSK$. La PSK es generada desde una *passphrase* (de 8 a 63 caracteres) o una cadena de 256-bit y proporciona una solución para redes domésticas o pequeñas empresas que no tienen servidor de autenticación,
- Si se usa un servidor de autenticación, la PMK es derivada de la MK de autenticación 802.1X.

La PMK en si misma no se usa nunca para la encriptación o la comprobación de integridad. Al contrario, se usa para generar una clave de encriptación temporal – para el tráfico unicast esta es la PTK (*Pairwise Transient Key*). La longitud de la PTK depende el protocolo de encriptación: 512 bits para TKIP y 384 bits para CCMP. La PTK consiste en varias claves temporales dedicadas:

- KCK (*Key Confirmation Key* – 128 bits): Clave para la autenticación de mensajes (MIC) durante el *4-Way Handshake* y el *Group Key Handshake*,
- KEK (*Key Encryption Key* – 128 bits): Clave para asegurar la confidencialidad de los datos durante el *4-Way Handshake* y el *Group Key Handshake*,
- TK (*Temporary Key* – 128 bits): Clave para encriptación de datos (usada por TKIP o CCMP),
- TMK (*Temporary MIC Key* – 2×64 bits): Clave para la autenticación de datos. Se usa una clave dedicada para cada lado de la comunicación.

El *4-Way Handshake*, iniciado por el punto de acceso, hace posible:

- confirmar que el cliente conoce la PMK,
- derivar una PTK nueva,
- instalar claves de encriptación e integridad,
- encriptar el transporte de la GTK,
- confirmar la selección de la suite de cifrado.

Se intercambian cuatro mensajes EAPOL-Key entre el cliente y el punto de acceso durante el *4-Way Handshake*.

La PTK se deriva de la PMK, una cadena fija, la dirección MAC del punto de acceso, la dirección MAC del cliente y dos números aleatorios (*ANonce* y *SNonce*, generados por el autenticador y el suplicante, respectivamente). El punto de acceso inicia el primer mensaje seleccionando el número aleatorio *ANonce* y enviándoselo al suplicante, sin encriptar el mensaje o protegerlo de las trampas. El suplicante genera su propio número aleatorio *SNonce* y ahora puede calcular la PTK y las claves temporales derivadas, así que envía el *SNonce* y la clave MIC calculada del segundo mensaje usando la clave KCK. Cuando el autenticador recibe el segundo mensaje, puede extraer el *SNonce* (porque el mensaje no está encriptado) y calcular la PTK y las claves temporales derivadas. Ahora puede verificar el valor de MIC en el segundo mensaje y estar seguro de que el suplicante conoce la PMK y ha calculado correctamente la PTK y las claves temporales derivadas.

El tercer mensaje enviado por el autenticador al suplicante contiene el GTK (encriptada con la clave KEK), derivada de un GMK aleatorio y *GNonce* (ver Figura 10), junto con el MIC calculado del tercer mensaje utilizando la clave KCK. Cuando el suplicante

recibe este mensaje, el MIC se comprueba para asegurar que el autenticador conoce el PMK y ha calculado correctamente la PTK y derivado claves temporales.

El último mensaje certifica la finalización del handshake e indica que el suplicante ahora instalará la clave y empezará la encriptación. Al recibirlo, el autenticador instala sus claves tras verificar el valor MIC. Así, el sistema móvil y el punto de acceso han obtenido, calculado e instalado unas claves de integridad y encriptación y ahora pueden comunicarse a través de un canal seguro para tráfico unicast y multicast.

El tráfico multicast se protege con otra clave: GTK (*Group Transient Key*), generada de una clave maestra llamada GMK (*Group Master Key*), una cadena fija, la dirección MAC del punto de acceso y un número aleatorio *GNonce*. La longitud de GTK depende del protocolo de encriptación – 256 bits para TKIP y 128 bits para CCMP. GTK se divide en claves temporales dedicadas:

- GEK (*Group Encryption Key*): Clave para encriptación de datos (usada por CCMP para la autenticación y para la encriptación, y por TKIP),
- GIK (*Group Integrity Key*): Clave para la autenticación de datos (usada solamente con TKIP).

Se intercambian dos mensajes *EAPOL-Key* entre el cliente y el punto de acceso durante el *Group Key Handshake*. Este handshake hace uso de claves temporales generadas durante el *4-Way Handshake* (KCK y KEK). El proceso se muestra en la Figura 11.

El Group Key Handshake sólo se requiere para la disasociación de una estación o para renovar la GTK, a petición del cliente. El autenticador inicia el primer mensaje escogiendo el número aleatorio *GNonce* y calculando una nueva GTK. Envía la GTK encriptada (usando KEK), el número de secuencia de la GTK y el MIC calculado de este mensaje usando KCK al suplicante. Cuando el mensaje es recibido por el suplicante, se verifica el MIC y la GTK puede ser desencriptada.

El segundo mensaje certifica la finalización del *Group Key Handshake* enviando el número de secuencia de GTK y el MIC calculado en este segundo mensaje. Al ser recibido este, el autenticador instala la nueva GTK (tras verificar el valor MIC).

También existe un *STakey Handshake*, pero no lo vamos a tratar aquí. Soporta la generación de una clave, llamada *STakey*, por el punto de acceso para conexiones ad-hoc.

La cuarta fase habla sobre la confidencialidad e integridad de datos RSNA. Todas las claves generadas anteriormente se usan en protocolos que soportan la confidencialidad e integridad de datos RSNA:

- TKIP (*Temporal Key Hash*),
- CCMP (*Counter-Mode / Cipher Block Chaining Message Authentication Code Protocol*),
- WRAP (*Wireless Robust Authenticated Protocol*).

Hay un concepto importante que debe ser entendido antes de detallar estos protocolos: la diferencia entre MSDU (*MAC Service Data Unit*) y MPDU (*MAC Protocol Data Unit*). Ambos términos se refieren a un sólo paquete de datos, pero MSDU representa a los datos antes de la fragmentación, mientras las MPDUs son múltiples unidades de datos tras la fragmentación. La diferencia es importante en TKIP y en el protocolo de encriptación CCMP, ya que en TKIP el MIC se calcula desde la MSDU, mientras que en CCMP se calcula desde MPDU.

Al igual que WEP, TKIP está basada en el algoritmo de encriptación RC4, pero esto es así tan sólo por un motivo: permitir a los sistemas WEP la actualización para instalar un

protocolo más seguro. TKIP se requiere para la certificación WPA y se incluye como parte de RSN 802.11i como una opción. TKIP añade medidas correctoras para cada una de las vulnerabilidades de WEP descritas anteriormente:

- Integridad de mensaje: un nuevo MIC (*Message Integrity Code*) puede ser incorporado en el software para microprocesadores lentos,
- IV: nuevas reglas de selección para los valores IV, reutilizando IV como contador de repetición (TSC, o *TKIP Sequence Counter*) e incrementando el valor del IV para evitar la reutilización,
- *Per Packet Key Mixing*: para unir claves de encriptación aparentemente inconexas,
- Gestión de claves: nuevos mecanismos para la distribución y modificación de claves.

TKIP Key-Mixing Scheme se divide en dos fases. La primera se ocupa de los datos estáticos – la clave TEK de sesión secreta, el TA de la dirección MAC del transmisor (incluido para prevenir colisiones IV) y los 32 bits más altos del IV. La fase 2 incluye el resultado de la fase 1 y los 16 bits más bajos del IV, cambiando todos los bits del campo *Per Packet Key* para cada nuevo IV. El valor IV siempre empieza en 0 y es incrementado de uno en uno para cada paquete enviado, y los mensajes cuyo TSC no es mayor que el del último mensaje son rechazados. El resultado de la fase 2 y parte del IV extendido (además de un bit dummy) componen la entrada para RC4, generando un flujo de clave que es XOR-eado con el MPDU de sólo texto, el MIC calculado del MPDU y el viejo ICV de WEP.

La computación del MIC utiliza el algoritmo Michael de Niels Ferguson. Se creó para TKIP y tiene un nivel de seguridad de 20 bits (el algoritmo no utiliza multiplicación por razones de rendimiento, porque debe ser soportado por el viejo hardware de red para que pueda ser actualizado a WPA). Por esta limitación, se necesitan contramedidas para evitar la falsificación del MIC. Los fallos de MIC deben ser menores que 2 por minuto, o se producirá una desconexión de 60 segundos y se establecerán nuevas claves GTK y PTK tras ella. Michael calcula un valor de comprobación de 8 octetos llamado MIC y lo añade a la MSDU antes de la transmisión. El MIC se calcula de la dirección origen (SA), dirección de la TMK apropiada (dependiendo del lado de la comunicación, se utilizará una clave diferente para la transmisión y la recepción).destino (DA), MSDU de sólo texto y CCMP se basa en la suite de cifrado de bloques AES (*Advanced Encryption Standard*) en su modo de operación CCM, con la clave y los bloques de 128 bits de longitud. AES es a CCMP lo que RC4 a TKIP, pero al contrario que TKIP, que se diseñó para acomodar al hardware WEP existente, CCMP no es un compromiso, sino un nuevo diseño de protocolo. CCMP utiliza el counter mode junto a un método de autenticación de mensajes llamado *Cipher Block Chaining* (CBC-MAC) para producir un MIC.

Se añadieron algunas características interesantes, como el uso de una clave única para la encriptación y la autenticación (con diferentes vectores de inicialización), el cubrir datos no encriptados por la autenticación. El protocolo CCMP añade 16 bytes al MPDU, 8 para el encabezamiento CCMP y 8 para el MIC. El encabezamiento CCMP es un campo no encriptado incluido entre el encabezamiento MAC y los datos encriptados, incluyendo el PN de 48-bits (*Packet Number* = IV Extendido) y la *Group Key KeyID*. El PN se incrementa de uno en uno para cada MPDU subsiguiente.

La computación de MIC utiliza el algoritmo CBC-MAC que encripta un bloque nonce de inicio (computado desde los campos de *Priority*, la dirección fuente de MPDU y el PN incrementado) y hace XORs sobre los bloques subsiguientes para obtener un MIC final de 64 bits (el MIC final es un bloque de 128-bits, ya que se descartan los últimos 64 bits). El MIC entonces se añade a los datos de texto para la encriptación AES en

modo contador. El contador se construye de un nonce similar al del MIC, pero con un campo de contador extra inicializado a 1 e incrementado para cada bloque.

El último protocolo es WRAP, basado también en AES pero utilizando el esquema de encriptación autenticada OCB (*Offset Codebook Mode – encriptación y autenticación en la misma operación*). OCB fue el primer modo elegido por el grupo de trabajo de IEEE 802.11i, pero se abandonó por motivos de propiedad intelectual y posibles licencias. Entonces se adoptó CCMP como obligatorio.

5. IEEE 802.1X, EAP y RADIUS

El protocolo de autenticación IEEE 802.1X (también conocido como *Port-Based Network Access Control*) es un entorno desarrollado originalmente para redes de cable, y posee mecanismos de autenticación, autorización y distribución de claves y además incorpora controles de acceso para los usuarios que se unan a la red. La arquitectura IEEE 802.1X está compuesta por tres entidades funcionales:

- el suplicante que se une a la red,
- el autenticador que hace el control de acceso,
- el servidor de autenticación que toma las decisiones de autorización.

En las redes inalámbricas, el punto de acceso sirve de autenticador. Cada puerto físico (puerto virtual en las redes inalámbricas) se divide en dos puertos lógicos, formando la PAE (*Port Access Entity*). La PAE de autenticación está siempre abierta y permite el paso de procesos de autenticación, mientras que el PAE de servicio sólo se abre tras una autenticación exitosa (por ejemplo, una autorización) por un tiempo limitado (3600 segundos por defecto). La decisión de permitir acceso está hecha por lo general por la tercera entidad, el servidor de autenticación (que puede ser un servidor Radius dedicado o – por ejemplo en las redes domésticas – un simple proceso funcionando en el punto de acceso).

El estándar 802.11i hace pequeñas modificaciones a IEEE 802.1X para que las redes inalámbricas estén protegidas frente al robo de identidades. La autenticación de mensajes se ha incorporado para asegurarse de que tanto el suplicante como el autenticador calculan sus claves secretas y activan la encriptación antes de acceder a la red.

El suplicante y el autenticador se comunican mediante un protocolo basado en EAP. El rol del autenticador es, esencialmente, pasivo – se limita a enviar todos los mensajes al servidor de autenticación. EAP es un entorno para el transporte de varios métodos de autenticación y permite sólo un número limitado de mensajes (*Request, Response, Success, Failure*), mientras que otros mensajes intermedios son dependientes del método seleccionado de autenticación: EAP-TLS, EAP-TTLS, PEAP, Kerberos V5, EAP-SIM etc. Cuando se completa el proceso (por la multitud de métodos posibles), ambas entidades (suplicante y servidor de autenticación) tendrán una clave maestra secreta. El protocolo utilizado en las redes inalámbricas para transportar EAP se llama EAPOL (EAP Over LAN), las comunicaciones entre autenticador y servidor de autenticación utilizan protocolos de capa más alta, como Radius, etc.

El protocolo Extensible Authentication Protocol (EAP) es un protocolo de autenticación flexible, que es utilizado por el estándar IEEE 802.1X de control de acceso en las LANs. Entre los diferentes métodos de autenticación se encuentran:

- **EAP-MD5:** es la versión menos segura del protocolo EAP, utiliza el nombre de usuario y contraseña para realizar la autenticación, usando la función hash MD5 de la

contraseña para la verificación. Al no comprobar la identidad del servidor es muy vulnerable a ataque del tipo Man-in-the-Middle.

- **EAP-LEAP:** es un sistema EAP propietario de Cisco. Al igual que la versión MD5, utiliza el nombre de usuario y contraseña para realizar la autenticación. Como servidor de autenticación utiliza un servidor RADIUS (explicado en apartados posteriores). Utiliza autenticación mutua para evitar ataques Man-in-the-Middle como en el caso anterior.

- **EAP-TLS:** usa certificados X.509 tanto para el usuario como para el servidor para la autenticación mutua y el cifrado de las comunicaciones. Este sistema permite una autenticación con un nivel de seguridad muy alto, pero necesita la generación de certificados para todos los usuarios, lo cual puede ser un inconveniente para organizaciones pequeñas.

- **EAP-TTLS / PEAP:** en estas versiones se elimina la necesidad del certificado por parte del usuario necesario en el caso de la versión TTLS. La identidad del servidor se establece usando su certificado y la de usuario mediante un nombre de usuario y contraseña usando un servidor RADIUS.

- **EAP-SIM:** especifica un mecanismo para la autenticación mutua y acuerdo de llave de sesión usando GSM-SIM (Global System for Mobile Communications - Subscriber Identity Modules) y proponiendo un realce a los procedimientos de autenticación de GSM. Desafortunadamente, este no es exitoso en su finalidad de proveer seguridad de 128 bit de los actuales 64 bit de GSM. Además, este no provee independencia de sesión entre diferentes sesiones. Para el primer problema se pueden buscar soluciones, pero el segundo no tiene solución en la práctica.

- **Kerberos:** es un protocolo de seguridad desarrollado en el Instituto de Tecnología de Massachusetts (MIT), para autenticar usuarios y clientes en una red, y distribuir claves de encriptación, de forma segura. Permite que entidades que se comunican a través de una red, puedan probar su identidad, evitando que puedan ser suplantadas. También proporciona capacidades de integridad de datos (detección de modificaciones) y seguridad de datos (para evitar lecturas no autorizadas) usando sistemas criptográficos como DES.

Kerberos funcionan proporcionando a los participantes (usuarios o servicios) “tickets” digitales, que pueden usar para identificarse en la red y como clave criptográfica para hacer las comunicaciones de forma segura.

El Remote Authentication Dial-In User Service (RADIUS) es un sistema de autenticación y control de usuarios usado por muchos proveedores de acceso a Internet. Actualmente RADIUS forma parte de los mecanismos de seguridad del protocolo EAP (comentado anteriormente). El servidor RADIUS es el encargado de validar el acceso de los usuarios de forma centralizada usando nombres de usuario y contraseña. El cliente que desea conectarse a la red wireless utiliza alguna de las variantes para autenticarse. Dicha petición EAP llega al punto de acceso el cual se encargará de transmitir la petición al servidor RADIUS, el cual se encarga de validar al usuario, usando su nombre de usuario y contraseña o su certificado. El resultado de la validación es devuelto al cliente wireless, aceptando o denegando el acceso.

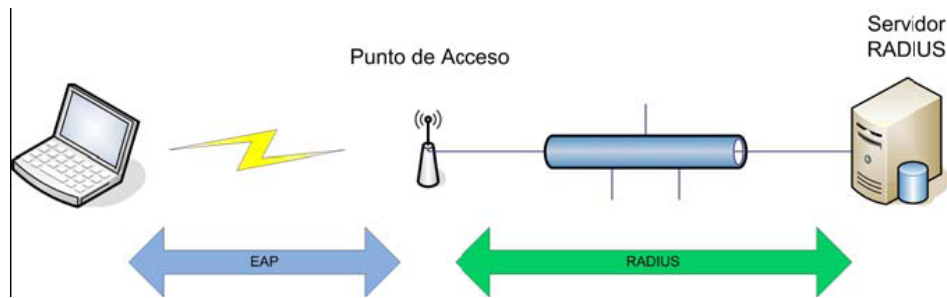


Figura 7. Autenticación EAP con RADIUS. [SEGRI]

Algunos puntos de acceso permiten realizar filtrados de MAC usando servidores RADIUS, de manera que la MAC de la máquina que desea conectarse a la red wireless debe pasar por el servidor para ser validada.

6. Referencias

- [INSEG] Oliva Fora, Pau. “(In)seguridad en redes 802.11b”.
- [SEGWF] Lehembre, Guillaume. “Seguridad Wi-Fi – WEP, WPA y WPA2”.
- [SEGRI] de Alfonso, Carlos - Caballer, Miguel – Hernández, Vicente. “Seguridad en Redes Inalámbricas”.

7. Bibliografía

- [1] FARMER, VENEMA. Improving the security of your site by breaking into it. Sun Microsystems y Eindhoven University of Technology. Recuperado el 29 de febrero de 2004 de <http://www.fish.com/satan/admin-guide-to-cracking.html>
- [2] Ptacek, Thomas H. y Newsham, Timothy N. Insertion, evasion and denial of service: eluding network intrusion detection. Recuperado el 26 de febrero de 2004 de <http://www.securityfocus.com/data/library/ids.ps>
- [3] Oliva Fora, Pau. (In)seguridad en redes 802.11b. Recuperado el 10 de Agosto de 2006 de <http://www.matarowireless.net>
- [4] Australian Computer Emergency Response Team. Recuperado el 30 de Septiembre de <http://www.auscert.org.au>
- [5] US-CERT. United States Computer Emergency Readiness Team. Recuperado el 30 de Septiembre de 2006 de <http://www.kb.cert.org>
- [6] Lehembre, Guillaume. Seguridad Wi-Fi – WEP, WPA y WPA2. Recuperado el 9 de Octubre de 2006 de http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf
- [7] de Alfonso, Carlos - Caballer, Miguel – Hernández, Vicente. Seguridad en Redes Inalámbricas. 2005. Recuperado el 11 de Octubre de www.dsic.upv.es/docs/bib-dig/informes/etd-06242005-121243/DSIC-II-04-05.TechReport.pdf
- [8] Wu, T., "A Real-World Analysis of Kerberos Password Security". Stanford University Computer Science Department.
- [9] Aboba, Bernard – Palekar, Ashwin. IEEE 802.1X and RADIUS Security. Recuperado el 12 de Octubre de 2006. <http://www.drizzle.com/%7Eaboba/IEEE/11-01-TBD-I-RADIUS-Security.ppt>
- [10] The Unofficial 802.11 Security Web Page. Recuperado el 11 de Octubre de 2006. <http://www.drizzle.com/%7Eaboba/IEEE/>
- [11] An inicial security análisis of the IEEE 802.1X Standard. Recuperado el 10 de Enero de 2007. <http://www.cs.umd.edu/%7Ewaa/1x.pdf>

- [12] Unsafe at any key size; An Analysis of the WEP encapsulation. Recuperado el 11 de Enero de 2007.
<http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip>