

Vulnerabilidades en 802.11

Giovanni Zuccardi
Juan David Gutiérrez

Octubre de 2006

Contenido

1. Definición
2. Deficiencias de WEP
 - a. MIC Independiente de la llave
 - b. Tamaño de IV demasiado corto
 - c. Reutilización el IV
 - d. Deficiencias del RC4
3. Deficiencias en el método Shared Key
4. Debilidad ACL(Access Control List)
5. FreeBSD - IEEE 802.11 Buffer Overflow
6. Denegación del servicio en IEEE 802.11
7. Debilidades en 802.11i (WPA2)
 - a. Vulnerabilidad contra la clave PSK
 - b. Vulnerabilidad de denegación del servicio
 - c. Vulnerabilidad en el Temporal Key Hash
8. Debilidades EAP
 - a. Vulnerabilidad en Kerberos
 - b. Vulnerabilidad en el LEAP de Cisco
 - c. Vulnerabilidad de RADIUS
9. Debilidades del estándar IEEE 802.1X
 - a. Ausencia de autenticación mutua
 - b. Debilidad de EAP de mensaje satisfactorio
 - c. Secuestro de sesión
10. Referencias
11. Bibliografía

Vulnerabilidades en 802.11

1. Definición

Hoy en día, Internet ha facilitado y promovido el desarrollo de las comunicaciones a nivel global. Esto ha llevado a la creación de nuevas redes y de herramientas para compartir información a través de ella.

Lo anterior ha permitido el surgimiento en las empresas del rol administradores de red, los cuales velan por el uso correcto de la red y deben satisfacer unas necesidades de seguridad y confidencialidad de la información manejada en dichas redes.

Sin embargo, los ataques a la red o a computadores conectados a ella siguen aumentando cada día. El nivel de sofisticación de estos es cada vez mayor, lo cual exige el desarrollo y actualización de herramientas pertinentes.

Es notable la gran importancia de desarrollar mecanismos de autoprotección contra los diferentes tipos de ataques, que brinden la identificación de riesgos potenciales, análisis de debilidades para después acciones de mejora y defensa así como mitigación de sucesos indeseables.

Las vulnerabilidades en un sistema surgen de los errores individuales de un componente, aunque pueden surgir nuevas vulnerabilidades con más complejidad a partir de la interacción de componentes (sistema de archivos, kernel del sistema, servidores de procesos, etc.). Actualmente existen programas diseñados para detectar y analizar vulnerabilidades llamados analizadores de vulnerabilidades. Los analizadores de vulnerabilidades mas usados actualmente son el Nessus, Satan, N-Stealth, Nikto y los llamados ISS (Internet Security Scanner) y SSS (System Security Scanner).

Enfocándonos en las redes inalámbricas se puede decir que la principal vulnerabilidad de una red inalámbrica es el hecho que cualquier persona puede acceder los datos que transitan por la red, debido a que no existe ningún medio físico que imposibilite el acceso.

2. Deficiencias de WEP

La estación receptora en WEP únicamente aceptará un mensaje si el ICV (Integrity Check Value) 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 lineares: $CRC(m \oplus k) = CRC(m) \oplus CRC(k)$

Debido a que los CRCs son lineares, se puede generar un ICV valido ya que el CRC se combina con una operación XOR que también es linear y esto permite hacer el '*bit flipping*' como veremos a continuación:

- Un atacante debe interceptar un mensaje m (conocido o no) y modificarlo de forma conocida para producir m':

$$m' = m \oplus \Delta$$

- Como el CRC-32 es lineal, puede generar un nuevo ICV' a partir del ICV de m:

$$ICV' = ICV \oplus h(\Delta)$$

- ICV' será valido para el nuevo cyphertext c'

$$c' = c \oplus \Delta = k \oplus (m \oplus \Delta) = k \oplus m'$$

Todo este proceso se puede resumir en la siguiente grafica:

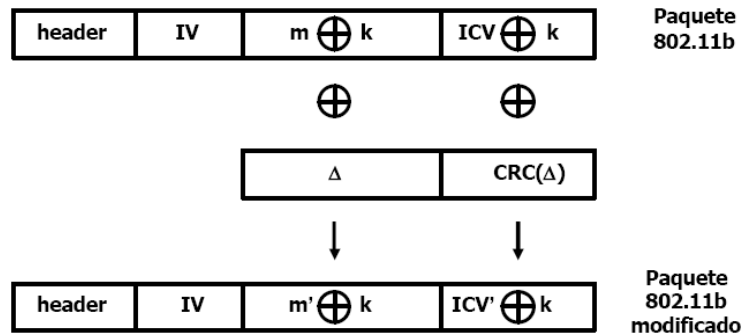


Figura 3: Modificación de un paquete. [INSEG]

a. MIC Independiente de la llave

Esta vulnerabilidad WEP es conocida como Ausencia de mecanismo de chequeo de integridad del mensaje (MIC) dependiente de la llave (Lack of keyed MIC).

El MIC que utiliza WEP es un simple CRC-32 calculado a partir del payload, por lo tanto no depende de la llave ni del IV. Esta debilidad en la encriptación da lugar a que conocido el plaintext de un solo paquete encriptado con WEP sea posible inyectar paquetes a la red.

Esto es posible de la siguiente manera:

- El atacante captura un paquete $c = m \oplus k$ donde m es conocido (por ejemplo, el atacante envía un e-mail a la victima)

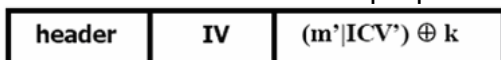
- El atacante recupera el flujo pseudo-aleatorio $k = c \oplus m$ para el IV concreto del paquete.

- Supongamos que el atacante quiere inyectar un mensaje m', debe realizar lo siguiente:

$$ICV' = CRC32(m')$$

- El atacante ya puede ensamblar la parte encriptada del paquete: $c = (m'|ICV') \oplus k$

- El atacante obtiene un paquete válido y listo para ser inyectado a la red:



b. Tamaño de IV demasiado corto

El vector de inicialización (IV) tiene sólo 24 bits de longitud (sin encriptar). Matemáticamente sólo hay 2^{24} (16.777.216) posibles valores de IV. Aunque esto pueda parecer mucho, 16 millones de paquetes pueden generarse en pocas horas en una red wireless con tráfico intenso.

La corta longitud del IV, hace que éste se repita frecuentemente y de lugar a la deficiencia del protocolo que veremos a continuación, basada en la

posibilidad de realizar ataques estadísticos para recuperar el plaintext gracias a la reutilización del IV.

c. Reutilización el IV

Si un IV se repite, se pone en riesgo la confidencialidad. WEP no usa RC4 con cuidado. El estándar 802.11 especifica que cambiar el IV en cada paquete es opcional.

El IV normalmente es un contador que empieza con valor cero y se va incrementando de uno en uno, por lo tanto:

- Rebotar causa la reutilización de IV's
- Sólo hay 16 millones de IV's posibles, así que después de interceptar suficientes paquetes, seguro que hay IV's repetidos.

Un atacante capaz de escuchar el tráfico 802.11 puede descifrar ciphertexts interceptados incluso sin conocer la clave.

d. Deficiencias del RC4

El uso de RC4 por WEP es cuestionable, ya que este algoritmo tiene sus propias deficiencias, la más importante es la incapacidad de generar acceso aleatorio. Otro problema de RC4 es que una de cada 256 llaves es débil, esto quiere decir que esta menos correlacionada que como debería estar, por lo cual es mucho más fácil de analizar su contenido cifrado. Por último, el uso continuo de las llaves RC4 muestra una diagonal medible empíricamente, es decir que oculta imperfectamente los datos correlacionados.

3. Deficiencias en el método Shared Key

La principal deficiencia de este método consiste en la posibilidad de adivinar la llave compartida (Shared Key). Únicamente es necesario usar la primera palabra de un keystream, para poder obtener información de la clave secreta compartida.

El procedimiento consiste en buscar IVs que causen que no haya información de la llave en el keystream. Los autores llamaron a esta condición "resolved condition" o condición resuelta. Cada uno de estos paquetes resueltos sólo tiene ausencia de información de un byte de la llave, y este byte debe ser adivinado correctamente para que el siguiente paquete pueda ofrecer información del siguiente byte de la llave. Para realizar el ataque más rápidamente sólo se buscan los IVs débiles que cumplen esta condición. Hay una posibilidad del 5% de adivinar el byte de la llave correctamente cuando encontramos un paquete resuelto (con un IV débil). Pero como hay gran cantidad de paquetes resueltos viajando por la red, las posibilidades son aún mayores.

4. Debilidad ACL (Access Control List)

Una de las medidas más comunes que se utilizan para darle más seguridad a una red inalámbrica es restringir las máquinas que podrán comunicarse con el Punto de Acceso haciendo filtrado por dirección MAC en éste. Para esto se suele crear una tabla en el punto de acceso que contiene todas las MACs de los clientes que están autorizados para conectar. Aunque esto pueda parecer una medida de seguridad efectiva, no lo es, ya que es muy fácil cambiar la dirección MAC que aparece en los paquetes que un cliente

envía, y hacernos pasar por uno de los equipos que si que tienen acceso a la red.

5. FreeBSD - IEEE 802.11 Buffer Overflow

El subsistema FreeBSD en redes 802.11 implementa el protocolo de negociación usado en redes inalámbricas. Esta vulnerabilidad se produce por un desbordamiento de un integer en el manejador de paquetes corruptos tipo Beacon o Probe Response en IEEE 802.11 cuando un escaneo en busca de redes existentes resulta en un paquete que desborda el buffer. Esto permite a un atacante realizar un paquete Beacon o Probe Response a mano muy cuidadosamente y enviarlo a todas las estaciones, con la posibilidad de ejecutar código arbitrario dentro del contexto del FreeBSD kernel de un sistema escaneando por redes inalámbricas.

Para solucionar esta vulnerabilidad se debe instalar un patch y compilar el kernel otra vez.

6. Denegación del servicio en IEEE 802.11

Esta vulnerabilidad existe en la implementación del hardware del protocolo inalámbrico IEEE 802.11 que permite un trivial pero efectivo ataque en contra de la disponibilidad de dispositivos en una red de área local inalámbrica (WLAN).

Un atacante usando un dispositivo de bajo consumo como una PDA y una tarjeta de red inalámbrica puede causar una interrupción significativa de todo el tráfico de la Wlan dentro del rango, por ello se dificulta la identificación y localización del atacante.

Esta vulnerabilidad se encuentra relacionada con la MAC del protocolo IEEE 802.11. Dispositivos inalámbricos que realizan CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) que minimiza la transmisión de dos dispositivos simultáneamente. El uso del procedimiento CCA (Clear Channel Assessment) usado en todo hardware basado en el estándar y realizado por la capa física en DSSS (Direct Sequence Spread Spectrum). Un atacante usa la funcionalidad del CCA en la capa física y causa a todos los nodos Wlan dentro del rango (AP y Clientes) y difiere la transmisión de los datos durante la duración del ataque. Durante el ataque el dispositivo se comporta como si el canal estuviera siempre ocupado, impidiendo la transmisión de cualquier dato.

Antes, los ataques de disponibilidad requerían hardware especializado y dependían de la habilidad de saturar la frecuencia de la red con radiación de alto poder. Esta vulnerabilidad hace exitoso un ataque de bajo costo realizado por un atacante con habilidades promedio.

Esta vulnerabilidad afecta hardware de dispositivos inalámbricos que implementan IEEE 802.11 usando DSSS en la capa física. Incluyendo dispositivos IEEE 802.11, 802.11b, 802.11g de baja velocidad (por debajo de 20Mbps) y excluyendo IEEE 802.11a y 802.11g de alta velocidad.

El impacto de este ataque se encuentra dentro del alcance del dispositivo atacante, si un access point esta dentro el rango, todas las estaciones asociadas a él, serán afectadas.

El ataque puede ser montado usando hardware y drivers comunes. El ataque consume pocos recursos en dispositivos de ataque, lo que lo hace poco costoso. Esta vulnerabilidad no será mitigada por incrementos de seguridad

de la capa MAC de emergencia como IEEE 802.11 TG. Porque se pueden seguir enviando paquetes EAPOL-Logoff, EAPOL-Start o consumiendo todo el espacio de identificación EAP (EAP Identifier space 0-255), enviando un paquete anticipado de EAP satisfactorio, un paquete EAP modificado o suplantación de paquetes EAP fallidos. Por último, varios vendedores han confirmado que no hay una forma de defenderse de este ataque en WLAN basadas en DSSS.

No existe una forma de mitigación con respecto a actualización de software o firmware, ya que es un problema inherente de la implementación del protocolo IEEE 802.11 DSSS. Los efectos de este ataque no son persistentes, es decir una vez termine la congestión en la transacción, la recuperación de la red es inmediata.

7. Debilidades en 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.

a. Vulnerabilidad contra la clave PSK

La vulnerabilidad más práctica es el ataque contra la clave PSK de WPA/WPA2. Como ya hemos dicho, la PSK proporciona una alternativa a la generación de 802.1X PMK usando un servidor de autenticación. Es una cadena de 256 bits o una frase de 8 a 63 caracteres, usada para generar una cadena utilizando un algoritmo conocido: $PSK = PMK = PBKDF2(\text{frase}, SSID, SSID \text{ length}, 4096, 256)$, donde PBKDF2 es un método utilizado en PKCS#5, 4096 es el número de hashes y 256 la longitud del resultado. La PTK es derivada de la PMK utilizando el *4-Way Handshake* y toda la información utilizada para calcular su valor se transmite en formato de texto.

La fuerza de PTK radica en el valor de PMK, que para PSK significa exactamente la solidez de la frase.

El segundo mensaje del *4-Way Handshake* podría verse sometido a ataques de diccionario o ataques offline de fuerza bruta.

El diseño del protocolo (4096 para cada intento de frase) significa que el método de la fuerza bruta es muy lento (unos centenares de frases por segundo con el último procesador simple). La PMK no puede ser precalculada (y guardada en tablas) porque la frase de acceso está codificada adicionalmente según la ESSID. Una buena frase que no esté en un diccionario (de unos 20 caracteres) debe ser escogida para protegerse eficazmente de esta debilidad.

b. Vulnerabilidad de denegación del servicio

La otra debilidad WPA es una posibilidad de Negación del Servicio durante el *4-Way Handshake*. Debido a que el primer mensaje del *4-Way Handshake* 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 (denegación del servicio) sobre el cliente si es posible que existan varias sesiones simultáneas.

c. Vulnerabilidad en el Temporal Key Hash

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 (de 2^{128} a 2^{105}) bajo ciertas circunstancias. 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.), 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 interceptación de frecuencias de radio, Negación del Servicio a través de violaciones de 802.11, de-autenticación, de-asociación, etc.

8. Debilidades EAP

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).

a. Vulnerabilidad en Kerberos

Kerberos IV y V son vulnerables a ataques con diccionario. Estos ataques son particularmente potentes cuando se llevan a cabo en un lugar donde un gran número de intercambios de autenticación pueden ser recolectados en un corto tiempo, como en WLANs montadas en Hot Spots. Ataques de diccionario fuera de línea (offline) son fáciles de realizar contra el AS REP, mientras que la llave de encriptación del Kerberos ticket incluido sea una función de la contraseña. Estos ataques son favorables a la paralelización y por lo tanto es posible "crackear" un gran número de contraseñas en un corto tiempo con pocos recursos.

Kerberos V no debería ser usado sin extensiones que provean protección contra ataques de diccionario fuera de línea. Se ha propuesto que la vulnerabilidad de ataque de diccionario en Kerberos V sea mitigada con un

intercambio de pre-autenticación o mediante el uso de una autenticación de llave pública

b. Vulnerabilidad en el LEAP de Cisco

Cisco LEAP (Lightweight EAP) es un algoritmo de autenticación mutua que soporta derivación dinámica de llaves de sesión. La autenticación mutua depende de un secreto compartido, la contraseña de usuario, que es conocida por el cliente y la red, y es usada para responder a desafíos entre el usuario y el servidor RADIUS (Remote Authentication Dial-In User Service). Como todos los algoritmos basados en contraseñas, Cisco LEAP es vulnerable a ataques de diccionario. Durante un ataque de diccionario, variaciones de contraseñas son usadas para comprometer las credenciales de autenticación del usuario.

Cisco desarrollo EAP-FAST (EAP-Flexible Authentication via Secure Tunneling) para usuarios que desean montar una 802.1x EAP que no requiera certificados digitales y no es vulnerable a ataques de diccionario.

La política de crear una contraseña muy fuerte es la forma más efectiva de mitigar ataques de diccionario. Los usuarios también pueden migrar a otros tipos de EAP como EAP-FAST, PEAP o EAP-TLS que no son vulnerables a ataques de diccionario.

c. Vulnerabilidad de RADIUS

- Ataque de diccionario fuera de línea en RADIUS Shared Secret.
Muchas implementaciones solo permiten shared-secret que sean caracteres ASCII, y menos de 16 caracteres, lo que conlleva a shared secret con entropía baja. También un atacante puede capturar paquetes Access-Request/Response, Accounting-Request o Accounting-Response para un ataque de diccionario fuera de línea. El estado MD5 puede ser pre-computarizado entonces los ataques de diccionario son eficientes.
Un atacante puede intentar un ataque fuera de línea en cualquier paquete con un atributo EAP-Message. El uso de HMAC-MD5 en el atributo EAP-Message hace el ataque más difícil, entonces el Response Authenticator es el enlace débil.
- Descifrado de atributos ocultos en tiempo
Un atacante autenticado vía PAP, mediante la recolección de paquetes RADIUS Access-Request, puede determinar el keystream usado para proteger el atributo User-Password. También permite la recolección de Request Authenticators/IDs y el correspondiente keystream. Con los keystream capturados, el atacante puede generar nuevos keystream para cada valor Salt. Mientras más valores tabulados de RA/ID/Salt la descifrado en tiempo real de los atributos User-Password, Tunnel-Password, MPPE-Key es más factible.
- Ataques de texto plano conocidos contra Tunnel-Password
Un atacante crackeando un User-Password puede enviar un Access-Request elaborado y recibir de regreso un Access-Response con el atributo tunnel password y el Salt. Mientras el MD5 (Secret+RA) sea conocido, así como el Salt, es posible calcular inmediatamente el MD5(Secret+RA+Salt) y el Tunnel-Password está inmediatamente comprometido.

9. Debilidades del estándar IEEE 802.1X

La IEEE ha propuesto una arquitectura como solución a largo plazo a todas las fallas de seguridad presentes en 802.11, la cual es llamada RSN (Robust Security Network), la cual usa el estándar 802.1X como base para el control de acceso, autenticación y administración de llaves. Aunque esta solución presenta hasta el momento dos problemas de seguridad (el secuestro de sesión y la posibilidad de realizar Man in the Middle).

a. Ausencia de autenticación mutua

La falta de autenticación mutua entre la estación y el access point es uno de los problemas de seguridad presentes en esta arquitectura, ya que la autenticación de una vía entre la estación y el access point puede exponer a la estación a un potencial ataque Man in the Middle con un atacante actuando como un access point hacia la estación y como una estación hacia el access point de la red. Cualquiera llegaría a pensar que el punto débil de esta arquitectura son los access point, lo cual es erróneo, toda la arquitectura se torna insegura si las capas superiores del protocolo también aplican autenticación de una vía. La siguiente figura ilustra la configuración del ataque:

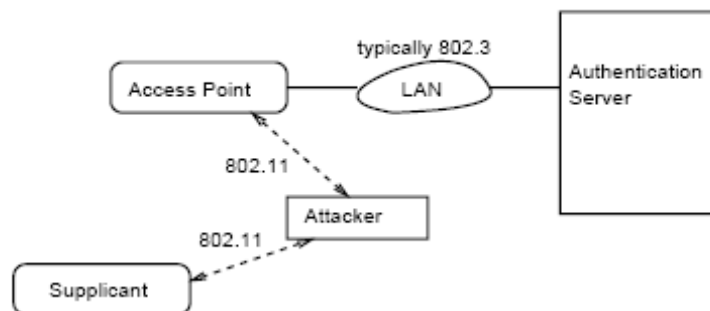


Figura 8: Configuración del ataque Man in the Middle. [802.1X]

b. Debilidad de EAP de mensaje satisfactorio

Un mensaje de satisfactorio es enviado desde el autenticador hacia la estación, cuando se recibe un mensaje de acceso aceptado RADIUS del servidor de autenticación RADIUS, esto indica que la autenticación ha sido exitosa. Sin importar el método de autenticación superior, este mensaje no contiene información para la preservación de la integridad. Como también sucede en la estación suplicante, la cual tiene una condición de cambio al estado autenticado sin importar cual sea el estado anterior. El mensaje satisfactorio EAP cambia el valor de la casilla eapSuccess, la cual hace un cambio inmediato al estado autenticado y esto normalmente producirá conectividad a la red.

Teniendo en cuenta esto, un atacante puede forjar un paquete representando al autenticador, empezando un potencial y sencillo ataque Man in the Middle.

c. Secuestro de sesión

Con IEEE 802.1X, la autenticación de las capas superiores sucede después de la asociación/ reasociación del RSN, por lo cual hay dos máquinas de estados, el RSN y 802.1X. La acción combinada de estas dos máquinas crean el estado de autenticación. Debido a la ausencia de comunicación

limpia entre estas dos maquinas y la autenticidad de los mensajes, es posible realizar un secuestro de sesión, aprovechando la falta de acoplamiento. El ataque tiene los siguientes pasos:

1. Mensajes 1, 2 y 3: Una estación legítima se autentica. La fase de autenticación EAP tiene más pasos, pero se ilustran tres por simplicidad.
2. Mensaje 4: Un atacante envía un paquete de disociación MAC 802.11 usando la dirección MAC del access point. Esto logra desasociar a la estación legítima. La transición de este mensaje deja a la maquina de estado del RSN en estado desasociado, mientras la maquina de estado 802.1X del autenticador permanece en estado autenticado.
3. Mensaje 5: El atacante gana acceso usando la dirección MAC de la estación legítima autenticada, ya que la maquina de estado 802.1X del autenticador permanece en estado autenticado.

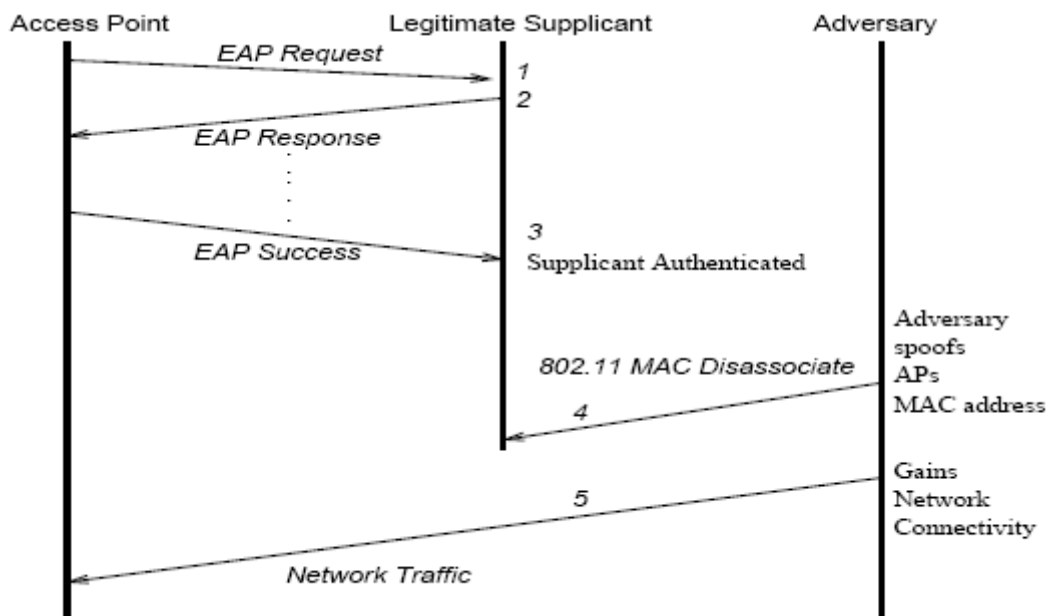


Figura 9: Secuestro de sesión mediante la imitación de un mensaje de disociación MAC 802.11. [802.1X]

10. 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".
- [802.1X] Mishra, Arunesh,- Arbaughi, William A.

11. 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.uscert.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>