Estudio de fortalezas y vulnerabilidades de los nuevos esquemas de autenticación en redes inalámbricas IEEE 802.11

Marcela Mejía Fajardo[1]

Ramiro A. Chaparro Vargas[2]

RESUMEN

El desarrollo de un nuevo esquema de confidencialidad y protección de información, en redes inalámbricas de área local IEEE 802.11 ha traído substanciales mejoras, incluyendo toda una nueva jerarquía de protocolos para satisfacer cada uno de los servicios de seguridad. Este artículo pretende analizar y determinar cuáles son aquellas fortalezas y vulnerabilidades presentes en el reciente modelo propuesto.

Palabras clave: 802.1X, Autenticación, EAP, RADIUS, Seguridad, WLAN.

Analysis of strengths and weaknesses of the new authentication schemes in wireless networks IEEE 802.11.

ABSTRACT

The recent development of new confidentiality and data protection schemes in wireless local area networks (WLAN) IEEE 802.11 has encouraged outstanding improvements, including a new protocol hierarchy, in order to satisfy each one of the security services. This paper pretends to establish and analyze which are the strengths and weaknesses of the recent proposed model.

Key words: 802.1X, Authentication, EAP, RADIUS, Security, WLAN.

1. INTRODUCCIÓN

Las redes inalámbricas cobran cada vez mayor importancia debido a sus múltiples aplicaciones, en especial aquellas orientadas a usuarios móviles. En particular, las redes inalámbricas de área local (WLAN) se están convirtiendo rápidamente en la arquitectura preferida en todo tipo de organizaciones comerciales, industriales, gubernamentales, educativas, de salud, de servicios, etc. Desafortunadamente, las WLAN aún presentan muchas vulnerabilidades en cuanto a seguridad. En el estándar IEEE 802.11 de 1999 [1], por ejemplo, este aspecto se cubrió muy rápidamente y de manera muy sucinta cuando se definió WEP como el esquema de seguridad a implementar dentro de una red de área local inalámbrica, sea ésta basada en infraestructura ó ad hoc. Pocos meses después de publicado el estándar apareció una gran cantidad de artículos en los que se mostraban todas las vulnerabilidades de WEP, las cuales le impiden proteger adecuadamente el acceso a los servicios y a la información de una red privada.

Posteriormente, en 2004, IEEE produjo el adendo IEEE 802.11i [2], donde se especifican los diferentes requerimientos para tener una red WLAN en la que cada usuario tenga una comunicación segura, ya sea con otros usuarios de la red ó con un servidor dentro de ésta. Nosotros, en particular, nos preocupamos por el aspecto de la autenticación, debido a los innumerables retos y oportunidades que este problema ofrece en el contexto de las redes inalámbricas IEEE 802.11.

El problema de la autenticación en WLAN basadas en infraestructura, se suele resolver mediante servidores de autenticación o entidades certificadoras ubicadas en el sistema de distribución, para lo cual se utilizan protocolos tales como el IEEE 802.1X. Aunque este protocolo no fue originalmente concebido para redes inalámbricas, se ajusta muy bien a las necesidades de las redes WLAN basadas en la infraestructura de un sistema de distribución.

De acuerdo con todo lo anterior, nuestro estudio estará centrado en los aspectos teóricos y prácticos asociados con el problema de la autenticación en las redes inalámbricas de área local, determinando con mayor precisión las fortalezas inherentes en los nuevos esquemas basados en servidores de autenticación RADIUS, protocolos de autenticación extensibles (EAP), robustos sistemas de administración de llaves y control de acceso por gestión

[1] Director del Grupo de Investigación WiNET en redes inalámbricas. Universidad Distrital.

[2] Director del Grupo de Investigación WiNET en redes inalámbricas. Universidad Distrital.

Artículo recibido el 25 de Abril de 2006. Aprobado para publicar el 29 de Junio de 2006.

de puertos; además, se describirá como estas propiedades han ofrecido nuevas herramientas para enfrentar las vulnerabilidades de esquemas de autenticación anteriores, gracias a sus características únicas. Basados en este estudio, deseamos exponer en primer lugar un análisis de operación y funcionamiento de estos esquemas, detallando los mecanismos empleados para la prestación integral de servicios tales como confidencialidad, autenticación, control de acceso e integridad en los datos. En segundo lugar, se expondrá un detallado compendio de fortalezas y vulnerabilidades en el empleo de los mecanismos, con el fin de describir las generalidades y especificaciones de está arquitectura de protocolos para la seguridad en tecnologías móviles, de tal forma que se puedan apreciar los alcances de este sistema no sólo desde el punto de vista del protocolo, sino también a partir de la misma implementación sobre equipos y escenarios reales.

En el desarrollo de este documento, la sección dos (2) comentará el modelo de autenticación vigente para la mayoría de las redes inalámbricas implementadas hoy en día, a fin de establecer en la sección tres (3) una comparación con el recientemente propuesto y adoptando esquema de autenticación basado en el protocolo 802.1X. En la sección cuatro (4) se definirá la relación entre el protocolo 802.1X como marco de trabajo para los verdaderos mecanismos de autenticación y protección de datos, soportados en el grupo de protocolos de autenticación extensibles EAP y RADIUS. Finalmente, en la sección cinco (5) y seis (6) se describirán los resultados y conclusiones que conlleva la implementación de uno u otro protocolo.

2. AUTENTICACIÓN EN IEEE 802.11

La autenticación busca confirmar la identidad del usuario destino, comprobando que éste sea quien dice ser ante los registros ó perfiles almacenados en la estación desde donde la información se origina [3]. Dicha verificación del usuario se maneja convencionalmente, por medio de otro servicio, denominado control de acceso, el cual se encarga de recibir ciertos parámetros sobre la identidad del cliente, como por ejemplo, un nombre de usuario y una contraseña, y a partir de allí utilizar estos datos para iniciar el proceso de autenticación.

En el caso concreto de las redes inalámbricas de área local, políticas de seguridad sustentadas en la capa física, es decir, limitación de puntos de conexión ó bloqueo de puertos de acceso a la red, se entienden como medidas poco eficaces para prevenir el acceso no autorizado a los recursos de la red, ya que el medio de transmisión es todo el espacio libre confinado dentro de la celda, lo cual redunda en la imposibilidad de establecer con precisión las fronteras en el área de cobertura de dicha celda. De acuerdo con esto la norma IEEE 802.11 permite únicamente la asociación de una estación a un punto de acceso (AP) ó a una estación igual en el caso de los IBSS (Independent Basic Service Set), si anteriormente se ha implementado el servicio de autenticación para el reconocimiento mutuo de los dos usuarios, en esta primera norma son dos los esquemas disponibles para la prestación de este servicio.

- Abierta: Desarrolla todo el proceso de autenticación en texto plano, es decir un intercambio de capacidades e identidades de la estación y el punto de acceso, sin llevarse a cabo una verificación del usuario ó la máquina. Sin embargo, es posible configurar el mecanismo de autenticación abierta para usar llaves WEP (Wired Equivalent Privacy); independiente de si la llave WEP es correcta ó incorrecta el usuario será asociado con el punto de acceso, pero si la llave es incorrecta quedará inhabilitado para transmitir ó recibir tramas, ya que todo mensaje vendrá encriptado con WEP. En resumen, la secuencia de transacción de la autenticación abierta cuenta con dos pasos: la transmisión de la identidad del usuario, junto con la solicitud de autenticación y la respuesta de aceptación.

- Llave Compartida: A diferencia, de la modalidad de autenticación anterior, en este mecanismo si se realiza una verificación del usuario ó la máquina en el otro extremo, pero para lograr esto es indispensable que tanto el punto de acceso como la estación compartan la misma llave WEP, ya que de lo contrario podrá negarse la autenticación del usuario a la unidad básica de servicios (BSS). La razón por la cual se debe compartir una llave WEP, es que una vez enviada la solicitud de autenticación por parte de la estación, el punto de acceso responderá con un desafío en texto plano que será encriptado con la llave WEP para ser devuelto al punto de acceso y a partir de su coincidencia ó no, se conceda el uso de los servicios de la red inalámbrica. En la Figura 1 es ilustrada la secuencia de transacciones.

Teniendo en cuenta el funcionamiento éstas dos (2) modalidades de autenticación, se han lle-

gado a detectar varias falencias, tales como el empleo de una única y muy corta llave para el cifrado de datos, denominada WEP. La ausencia total de un sistema de administración de llaves para prevenir la apropiación no autorizada de la llave WEP y por último una verificación no conjunta de desafío y usuario para la autorización del servicio. Con el fin, de resolver estos puntos se adoptó la utilización del protocolo 802.1X para la autenticación de usuarios y una nueva jerarquía de llaves en reemplazo de WEP.

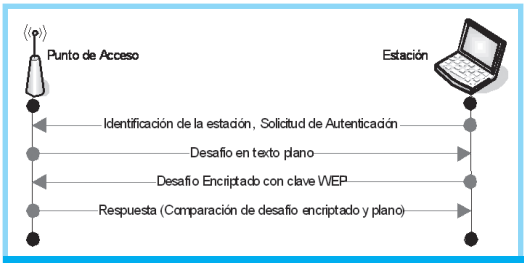

Figura 1. Secuencia de mensajes en autenticación con llave compartida

3. 802.1X Y SISTEMA DE ADMINISTRACIÓN DE LLAVES EN WLAN

El IEEE ha designado el protocolo 802.1X [4] como el marco de trabajo principal para el control de acceso y la distribución de llaves de seguridad, no sólo para redes inalámbricas IEEE 802.11 [5], sino también para todas las redes 802 en general. 802.1X es un mecanismo de control de acceso a la red basado en el manejo de puertos para la información de autenticación y autorización, donde el puerto representa la asociación de tipo controlada ó no controlada entre el usuario ó suplicante y el autenticador ó punto de acceso inalámbrico. Tanto el usuario suplicante como el punto de acceso operan sus mecanismos y protocolos de autenticación por medio de la entidad de puerto de acceso (PAE). Por su parte, el PAE del autenticador controla el estado de autorizado y no autorizado de su puerto controlado, dependiendo del resultado del proceso de autenticación; si el suplicante no ha sido autenticado aún, el punto de acceso utilizará su puerto no controlado para comunicarse con el PAE de éste, bloqueando todo tipo de tráfico y mensajes diferentes a los 802.1X. El protocolo adopta diversos mecanismos de autenticación EAP (Extensible Authentication Protocol), tales como TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security), PEAP (Protected EAP) y tarjetas inteligentes, gracias a los mensajes EAPOL (EAP over LAN), los cuales encapsulan los paquetes EAP entre el suplicante y el autenticador, quien finalmente lo enviará al servidor de autenticación en paquetes RADIUS (Remote Authentication Dial In User Service) ó cualquier otro tipo de servidor, dependiendo de la selección hecha. Para mayor detalle en la Figura 2 se ilustra la transacción completa de mensajes.

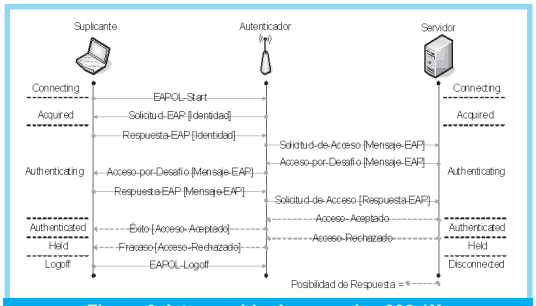

Figura 2. Intercambio de mensajes 802.1X

Se debe tener en cuenta que la autenticación 802.1X comienza tan pronto como el nodo móvil se ha asociado con el punto de acceso, mediante el establecimiento del estado de *Connecting* entre los PAE del suplicante y el autenticador. Este proceso dará inicio con el envío de una trama *EAPOL-Start* desde el nodo hacia el punto de acceso quien responderá con una solicitud de identidad para conocer el nombre usuario que requiere el acceso, éste estado se denomina *Acquired*. Procesado el mensaje por el usuario se enviará una respuesta hacia el autenticador para que este a la vez lo envíe hacia el servidor de autenticación, pasando así al estado *Authenticating*, durante este etapa se prepararán una serie de desafíos entre el servidor y el suplicante, donde el punto de acceso será únicamente un repetidor hasta que todos los requerimientos solicitados por el servidor sean satisfechos y se de autorización de acceso al usuario, en el estado de *Authenticated*. No obstante, el proceso puede finalizar con una negación del servicio debido al envío de información no concordante con lo solicitado, en este caso el estado del puerto será *Held* y notifica al usuario que el proceso de autenticación ha fracasado. Finalmente, para terminar con una sesión, cualquiera que haya sido el resultado se originará desde el usuario una trama *EAPOL-Logoff*, terminando el suplicante en el estado *Logoff* y el punto de acceso en *Disconnected*.

El protocolo IEEE 802.11i, presenta entre sus novedades un sistema de administración de llaves para la protección de sus mensajes, mediante los mecanismos de saludos de cuatro (4) vías y el saludo de llave de grupo. En comparación, con el protocolo original del IEEE, esta entrega supone un gran avance en materia de

El protocolo IEEE 802.11i, presenta entre sus novedades un sistema de administración de llaves para la protección de sus mensajes.

seguridad, dado que funciona sobre la base del protocolo IEEE 802.1X y que el intercambio de llaves entre los nodos no era examinada ni propuesta desde ningún punto de vista en el documento de 1999, sugiriendo incluso que fuese el administrador de red quien definiera sus propias políticas y protocolos de seguridad para el conocimiento conjunto de las llaves WEP a utilizarse entre los nodos de red. Ahora, se describirá en detalle los mecanismos de saludos, mencionados al comienzo del párrafo.

- Saludo de cuatro (4) vías: Este mecanismo tiene inicialmente cuatro (4) objetivos fundamentales por cumplir: confirmar la presencia de la comunicación entre un nodo y la red, garantizar la actualización periódica de las llaves de sesión, instalar la llave criptográfica y confirmar la instalación de la llave. El saludo puede llevarse a cabo gracias al formato de mensaje EAPOL-Key del protocolo IEEE 802.1X, el cual se especializa en el transporte de información criptográfica. En el saludo de cuatro (4) vías, el autenticador comienza por enviar al suplicante un mensaje que contiene información de la llave y un *Anonce*, es decir, un valor único de identificación para una llave, y cuya reasignación queda totalmente prohibida en el futuro; también se conoce como material de llave del autenticador. El suplicante al recibir el mensaje lo validará, mediante la inspección del contador de repeticiones, el cual se incrementa cada vez que un mensaje es enviado ó recibido, sólo en el caso tal, que este valor sea mayor al que se tiene establecido localmente, la transacción podrá continuarse normalmente, preparando hacia el autenticador un mensaje con el material de llave del autenticador (Anonce), un nuevo material de llave del suplicante (Snonce), la PMK* (Pairwise Master Key) y la PTK (Pairwise Transient Key) que es la derivación ó combinación pseudo-aleatoria de los tres parámetros anteriores. En la recepción de este segundo mensaje, el autenticador se encarga de validarlo, mediante la verificación del contador de repeticiones, y dependiendo del resultado de ésta operación, procederá a calcular por su cuenta la PTK, buscando una total concordancia con la PTK del suplicante, ya que su derivación se basa en los mismos parámetros de entrada. Si al comparar los resultados el autenticador halla la correspondencia, enviará un paquete hacia el suplicante con la información de llave, el *Anonce*, la información adicional de asociación ó reasociación e integridad de datos. El suplicante confirmará de nuevo la validez de este mensaje para finalmente enviar en un cuarto paquete la información de confirmación respecto a la llave, es decir, que el autenticador al recibir este mensaje dentro de la secuencia adecuada y con los campos de control correctos, entenderá que el suplicante ha instalado la PTK para el cifrado de datos, que de ahí en adelante utilizarán en el intercambio estos dos puntos.
- Saludo de llave de grupo: Dentro del sistema de administración de llaves existe adicionalmente éste mecanismo de saludo, cuyo principal objetivo es habilitar al autenticador para entregar una GTK (Group Transient Key) al suplicante, y así este último pueda recibir mensajes de difusión. El intercambio de mensajes el saludo de grupo siempre se producirá después del saludo de cuatro (4) vías e inicia con el envío de un mensaje desde el autenticador hacia el suplicante incluyendo información de la llave, la información de integridad de datos, la GTK (cifrada con la llave KEK ó *EAPOL-Key Encryption Key*) y la llave KCK (EAPOL-Key Confirmation Key); para que el suplicante pueda verificar la integridad del mensaje recibido con la KCK, debe desencriptar la GTK con la KEK y, si la comprobación de la integridad es exitosa el suplicante transmitirá un paquete final hacia el autenticador confirmando que tomará la GTK para el encriptado y desencriptado de mensajes en difusión.

Sin duda, una gran ventaja ofrecida por el protocolo 802.1X es la flexibilidad en el manejo de di versos mecanismos de autenticación entre el suplicante y el autenticador, dando cabida adicionalmente a una tercera entidad de autenticación, representada en un servidor RADIUS, quien con un protocolo independiente, pero ciento por ciento compatible y adaptable con EAP, permite aceptar ó denegar una solicitud de acceso basado en el mensaje y el usuario paralelamente.

4. MECANISMOS DE AUTENTICACIÓN Y RADIUS

Los mecanismos de autenticación EAP [6] y el protocolo RADIUS [7] se relacionan mediante un proceso de encapsulación de paquetes, es decir, el suplicante y el autenticador intercambian mensajes EAP y el autenticador retransmite estos mensajes hacia el servidor encapsulándolos en paquetes RADIUS [8]. El intercambio de mensajes desarrollado por la estación y el autenticador comienza con una solicitud de autenticación desde el punto de acceso hacia el usuario, el cual atenderá con un

mensaje de respuesta, donde le permite al autenticador conocer su identidad, éste pondrá en marcha su modo de operación de puente de paso para reenviar el mensaje hacia el servidor RADIUS, dentro de un paquete de *Solicitud de Acceso* con un atributo *Mensaje-EAP*. Una vez el servidor recibe este paquete responderá con un mensaje de *Acceso-por-Desafío* con su respectivo atributo EAP, que se encarga simplemente de encapsular la repuesta a aquella información que fue intercambiada inicialmente por el punto de acceso y el suplicante. El usuario para responder al desafío se respaldará con el autenticador para enviar un paquete *Respuesta-EAP* hacia el servidor y así finalmente después de una serie de intercambios opcionales de mensajes de desafíos llegar a una respuesta de rechazo ó aceptación del nodo móvil. Aunque pareciese que el punto de acceso no es más que un dispositivo pasivo de comunicación entre el usuario y el servidor, se presentan una serie de ventajas relevantes que revindican el uso de este equipo medio. La primera de ellas se relaciona con el establecimiento de una negociación previa entre el usuario y el autenticador para determinar si la solicitud el suplicante es procesable, es decir, si soporta EAP, si puede ser atendida localmente ó necesita ser enrutada hacia otro servidor e incluso si el mecanismo de autenticación EAP es aceptado por el usuario; el punto de acceso puede servir también como entidad central de registro para las transacciones realizadas entre diferentes usuarios y servidores de la misma celda [10]. Cualquier desacuerdo en la negociación del protocolo EAP entre el suplicante, autenticador y servidor arrojará un paquete *Rechazo-de-Acceso* al usuario.

5. IMPLEMENTACIÓN DE NUEVOS MECANISMOS DE AUTENTICACIÓN EN WLAN

El nuevo esquema de autenticación para redes inalámbricas de área local, según el estándar IEEE 802.11i, plantea la incorporación de un servidor RADIUS como nuevo elemento dentro de la red, para la autenticación centralizada de usuarios. Sin embargo, al momento de poner en marcha una topología de red de esta naturaleza, son varias las entidades adicionales que deben considerarse para garantizar una compacta arquitectura de seguridad. Para el desarrollo de este trabajo se dispuso una red inalámbrica sencilla, observada en la Figura 3 que nos permitiera reconocer y verificar el grado de seguridad obtenido con los mecanismos de autenticación EAP en conjunto con el protocolo RADIUS.

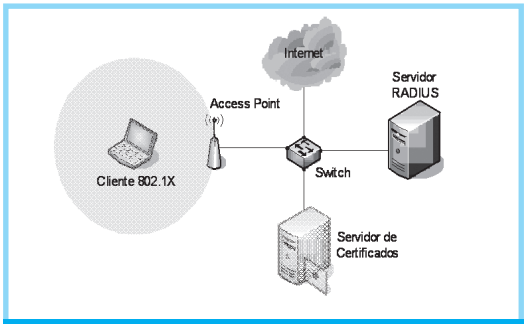

Figura 3. Escenario de pruebas

El escenario de pruebas consta de los (3) elementos principales enunciados por la norma: el suplicante (cliente 802.1X), el autenticador (access point) y servidor RADIUS. No obstante, es necesario en ciertos esquemas un servidor de certificados para algunos de los mecanismos de autenticación más robustos, por esta razón se muestra difuminado en la figura. Los mecanismos implementados y analizados son MD5, TLS, TTLS, PEAP y FAST [12], encontrando las siguientes fortalezas y vulnerabilidades en cada uno de ellos.

- MD5 (Message Digest 5) [13]: Es uno de los algoritmos más populares para la protección y cifrado de información, basado en la derivación de funciones hash; EAP lo emplea para brindar además de confidencialidad, también integridad de datos, generando desde el servidor a través de un módulo MD5 una secuencia binaria de 16 octetos, cuyas entradas son el código del mensaje RADIUS, el identificador, la longitud, el código autenticador, los atributos y el secreto compartido entre el autenticador y el servidor. La autenticación se completa cuando el cliente es capaz de resolver el desafío satisfactoriamente. Aunque debe aclararse que esté mecanismo en su estado nativo no es aplicable para las redes inalámbricas IEEE 802.11, dado que su autenticación es de una sola vía, es decir el autenticador ó access point será capaz de reconocer al cliente, pero el cliente jamás sabrá quien lo ha autenticado. Por lo tanto, la utilización de MD5 no es viable en WLAN, ya que el protocolo de referencia IEEE 802.11i establece que la autenticación entre entidades de la red debe ser mutúa, requerimiento no soportado por éste mecanismo de acuerdo a lo descrito. Entre algunas de las deficiencias propias del algoritmo se encuentra la incompatibilidad de EAP-MD5 para establecer sesiones con base en las llaves del sistema anfitrión, o sea, WLAN. El escenario de pruebas, contribuye a verificar que la

falla de este mecanismo no se produce en el servidor, ya que incluso éste envía un mensaje de aceptación a la solicitud de acceso, si el nombre de usuario y la contraseña son correctos. Por el contrario, el autenticador es quien denegará la solicitud al no recibir las llaves que le permitan establecer la sesión con el cliente, pero como se describirá más adelante existen formas de implementar este algoritmo, mediante conexiones preestablecidas por túnel.

- TLS (Transport Layer Security) [13]: Es uno de los protocolos de mayor familiaridad para los usuarios de Internet, ya que está basado en el mismo esquema que SSL (Secure Sockets Layer), ampliamente utilizado en transacciones Web seguras. El principio de funcionamiento de este mecanismo se basa en el establecimiento de un canal seguro entre el cliente y el servidor, aunque debe recordarse que el access point se encuentra de por medio, y es éste el único nodo de interés para el usuario 802.11, por este motivo dentro del proceso de establecimiento del canal TLS, al autenticador se le entregará el mismo material de llave para que construya sus propias herramientas de sesión, y así le sea transparente la comunicación entre cliente y servidor. A diferencia del algoritmo anterior, la implementación de EAP-TLS si requiere de la presencia de un servidor de certificados en la red, ya que tanto los clientes como el servidor necesitan tener instalados en sus sistemas las llaves públicas de sus extremos (certificado digital), para la autenticación mutua demandada por el estándar IEEE 802.11i. Desde el punto de vista de la implementación, el usuario no necesitará registrar ninguna contraseña y el servidor podrá prescindir de la misma en su base de datos de usuarios, ya que la transacción observada se basa en la manipulación de las credenciales de cada extremo que permiten el cifrado mediante llaves públicas de conocimiento extendido y el desencriptado por medio de las llaves privadas de conocimiento reservado. Las posibles vulnerabilidades de EAP-TLS, se pueden encontrar más en la administración de los elementos informáticos, que en el mismo desempeño del protocolo. Es decir, el manejo de las firmas digitales de los certificados deben ser respaldas por entidades certificadoras de amplio reconocimiento, ya que son las únicas con la potestad para validar la legítima propiedad de estos certificados entre los pares. Finalmente, se debe manejar con suficiente planeación el sistema de distribución de certificados entre los clientes de redes extendidas para la autorización de los nodos correctos.
- TTLS (Tunneled Transport Layer Security) [14]: Es un mecanismo de autenticación que pretende combatir las difíciles etapas de implementación de EAP-TLS, ya que no requiere que la autenticación mutua se fundamente en la posesión de certificados digitales en el extremo cliente y servidor. Como alternativa, el servidor se autenticará ante el cliente en primera instancia a través de su certificado digital para establecer el canal ó túnel seguro de comunicación entre los dos puntos y el cliente se autenticará ante éste con su contraseña ó credenciales, las cuales para esta etapa ya viajarán en un medio seguro mediante la implantación de un mecanismo interno de cifrado para toda la comunicación entrante y saliente del servidor RADIUS y el cliente. Durante la configuración, de los equipos que soportarían EAP-TTLS, se observó que es posible utilizar como mecanismos internos de cifrado, algoritmos y protocolos de autenticación de una sola vía, tales como PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), EAP-MD5, entre otros. Esto es posible, ya que la sesión ha sido protegida por el túnel. A pesar de contar con estas grandes fortalezas y facilidades el protocolo sólo podrá ser soportado por servidores cuyo sistema operativo sea Windows XP ó Windows 2000, restringiendo el uso de plataformas libres.
- PEAP (EAP Protegido): El mecanismo nace como una iniciativa conjunta de Cisco y Microsoft, se basa principalmente en el funcionamiento de EAP-TTLS y por ende de EAP-TLS, es decir, requiere del establecimiento de un canal seguro entre el cliente y el servidor, el cual será avalado mediante la instalación de certificados digitales, pero sólo en el extremo del servidor; el cliente por su parte llevará la autenticación en el sentido contrario a través del traspaso de sus credenciales. La diferencia de éste mecanismo con respecto a sus antecesores, radica en el mecanismo interior de cifrado de datos para el transporte de la información del cliente hacia el servidor, ya que PEAP sólo soporta algoritmos EAP y algoritmos propietarios de Cisco y Microsoft, tales como MS-CHAPv1, MS-CHAPv2 y GTC (Generic Token Card), exclusivo de Cisco. Restringiendo el uso de algoritmos propios PPP (Point to Point Protocol), como CHAP y PAP, aún soporta-

dos y utilizados por servidores RADIUS, igualmente se limita la diversidad de compatibilidad con software y hardware, diferente de Microsoft y Cisco. Finalmente, desde la óptica de la implementación PEAP y EAP—TTLS resultan ser protocolos prácticamente idénticos, dado que sus parámetros de configuración, sus requerimientos de recursos de una red de datos y sus políticas de intercambio de mensajes se mantienen inalterados.

FAST: Al implementar este mecanismo se conserva la protección de la comunicación entre el cliente y el servidor RADIUS mediante el establecimiento de un túnel de autenticación mutua con una sesión TLS. Con el fin, de asegurar dicho intercambio TLS, EAP-FAST hace uso de una credencial de acceso protegido (PAC), en lugar de implementar un servidor de certificados como se requiere en los mecanismos EAP-TTLS y PEAP. El funcionamiento de FAST se divide en tres (3) fases principalmente, en la primera el cliente envía una solicitud de autenticación al servidor con el mecanismo EAP-MS-CHAPv2 involucrado, si llega a determinarse que el usuario es válido, entonces un paquete RADIUS de rechazo (*Access-Reject*) será transmitido con un PAC vigente para el cliente; para la fase siguiente se hará uso del PAC por parte del cliente y el servidor en el establecimiento del túnel TLS de comunicación, a través del intercambio y reconocimiento mutuo de esta entidad. En la última fase, el servidor autentica al usuario utilizando EAP-GTC dentro del túnel TLS, de tal forma que la verificación correcta del PAC y las credenciales del usuario arrojen un mensaje de aceptación para el cliente (*Access-Accept*). Cabe aclarar que éste mecanismo durante su implementación requiere de adaptaciones en los mecanismos, que vayan de acuerdo con el hardware utilizado, ya que métodos MS-CHAPv2 y GTC son propietarios y no compatibles con plataformas diferentes a Microsoft y equipos Cisco. Algunas alternativas para ser configuradas son PAP y CHAP, como protocolos internos para el reemplazo de los anteriores.

6. CONCLUSIONES

El nuevo esquema de seguridad adoptado por las redes inalámbricas de área local IEEE 802.11 y sustentado en el adendo i, es en realidad el compendio y la definición de políticas de interoperabilidad entre diversos protocolos que cuentan con un reconocimiento previo y desempeño confiable para brindar los servicios de seguridad propios para la protección de datos y usuarios. Por lo tanto, la implementación de una red 802.11, cuyo sistema de seguridad se basa en esta jerarquía de protocolos, debe partir de un análisis y evaluación de aquellas condiciones aplicables al entorno inalámbrico, ya que se deben tener como prioridad la implementación de un sistema de administración de llaves, mecanismos de autenticación mutua y el establecimiento de canales seguros para el intercambio de la información correspondiente a los dos puntos anteriores. Sobre esta premisa debe clasificarse qué tan eficazmente se puede comportar el sistema de confidencialidad y privacidad implementado en una red inalámbrica de área local.

El nuevo esquema de seguridad es en realidad el compendio y la definición de políticas de interoperatibilidad entre diversos protocolos.

7. REFERENCIAS BIBLIOGRÁFICAS

[1] ANSI/IEEE Std. 802.11, «Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications». New York: IEEE Press, 1999.

[2] IEEE Std. 802.11i, «Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications». New York: IEEE Press, 2004.

[3] J.C. Chen, M.C. Jiang y Y. Liu, «Wireless LAN Security and IEEE 802.11i», Wireless Communications Magazine, Febrero 2005, pp. 27 – 36.

[4] IEEE Std. 802.1X – 2004, «IEEE Standard for local and metropolitan area networks Port – Based Network Access Control», New York IEEE Press, 2004.

[5] F. Bari y J.L. Bouthemy, «An AAA based service customization framework for public WLANs», *Wireless Communications and Networking Conference 2005*, Marzo 2005, pp. 2430 – 2435.

[6] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson y H. Levkowetz, «Extensible Authentication Protocol». IETF RFC 3748, Junio de 2004.

[7] C. Rigney, S. Willens, A. Rubens y W. Simpson, «Remote Authentication Dial In User Service (RADIUS)». IETF RFC 2865, Junio 2000.

[8] B. Aboba, y P. Calhoun, «RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)». IETF RFC 3579, Septiembre 2003.

[9] C. Zhuo, H. Fan y H. Liang, «A new authentication and key exchange protocol in WLAN», *Information Technology: Coding and Computing, 2005. ITCC 2005 International Conference*, Abril 2005, pp. 552 – 556.

[10] D. Mitton, M. St. Johns, S. Barkley, D. Nelson, B. Patil, M. Stevens y B. Wolf, «Authentication, Authorization and Accounting: Protocol Evaluation», IETF RFC 3127, Junio de 2001.

[11] A. Bakirdan, J. Qaddour y K. Jalozie. «Security algorithms in wireless LAN: propietary and nonpropietary», *IEEE Global Telecommunication Conference 2003*, Diciembre de 2003, pp. 1425 – 1429.

[12] R. Rivest, «The MD5 Message Digest Algorithm», IETF RFC 1321, Abril 1992.

[13] S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen y T. Wright, «Transport Layer Security Extensions», IETF RFC 4366, Abril de 2006.

[14] P. Funk y S. Blake-Wilson, «EAP Tunneled TLS Authentication Protocol (EAP-TTLS),» IETF Internet draft, Agosto 2003, trabajo en progreso.

Marcela Mejía Fajardo

Ingeniera electrónica, Universidad Santo Tomás. Magister en Teleinformática, Universidad Distrital Francisco José de Caldas. Actualmente se desempeña como profesora en el área de telemática y redes en el programa de ingeniería en telecomunicaciones de la Universidad Militar Nueva Granada de Bogotá, Colombia, y es directora e investigadora del grupo WiNET en redes inalámbricas. mmejiaf@umng.edu.co

Ramiro A Chaparro Vargas

Estudiante de último semestre de Ingeniería en Telecomunicaciones en la Universidad Militar Nueva Granada. Actualmente se encuentra desarrollando su proyecto de grado sobre mecanismos de autenticación en redes inalámbricas soportando servicios AAA, dentro del grupo de investigación WiNET. neosagan@ieee.org