ANÁLISIS DE DESEMPEÑO Y EVALUACIÓN DE REQUERIMIENTOS AAA EN PROTOCOLOS DE SEGURIDAD SOBRE REDES INALÁMBRICAS IEEE 802.11

ANALYSIS OF PERFORMANCE AND EVALUATION OF REQUIREMENTS AAA IN PROTOCOLS OF SECURITY ON RADIUS NETWORKS IEEE 802.11

Ramiro Alberto Chaparro Vargas [1]
Marcela Mejía Fajardo [2]

Fecha de Recepción: 31 de Agosto de 2006
Fecha de Aprobación: 22 de Octubre de 2006

RESUMEN: *El desarrollo de un nuevo esquema de confidencialidad y protección de información, en redes inalámbricas de área local IEEE 802.11 ha traído avances substanciales, incluyendo toda una nueva jerarquía de protocolos para satisfacer cada uno de los servicios de seguridad. Este artículo analiza y evalúa el desempeño y cumplimiento de requerimientos AAA de los protocolos RADIUS y DIAMETER, en entornos inalámbricos.*
PALABRAS CLAVES: *AAA, DIAMETRO, IEEE 802.11, RADIO, Seguridad, WLAN.*

ABSTRACT*: Confidentiality and data protection developments have led to an improved security framework for IEEE 802.11 wireless local area networks, including a new protocol hierarchy satisfying every privacy communications services. This article analyzes and evaluates RADIUS and DIAMETER standards, regarding their protocol performance and AAA requirements accomplishment in wireless environments.*
KEYWORDS: *AAA, DIAMETER, IEEE 802.11, RADIUS, Security, WLAN.*

1 Grupo de Investigación WiNET - Universidad Militar Nueva Granada2 Universidad Militar "Nueva Granada" GISSIC – gissic@umng.edu.co
2 Grupo de Investigación WiNET - Universidad Militar Nueva Granada2 Universidad Militar "Nueva Granada" GISSIC – gissic@umng.edu.co

I. INTRODUCCIÓN

Las redes inalámbricas de área local, debido a sus múltiples aplicaciones, cobran cada vez una mayor importancia, en especial aquellas orientadas a usuarios móviles. En particular, las redes inalámbricas de área local se están convirtiendo rápidamente en una alternativa eficiente y confiable para todo tipo de organizaciones comerciales, industriales, gubernamentales, educativas, de salud, de servicios, etc. No obstante, las redes inalámbricas de área local aún presentan muchas vulnerabilidades en cuanto a la seguridad. En el estándar IEEE 802.11 de 1999 [1], por ejemplo, este aspecto se cubrió ágilmente y de manera muy sucinta al definirse WEP (Wired Equivalent Privacy) como el esquema de seguridad a implementar dentro de una red de área local inalámbrica, bien sea una red de infraestructura o de igual a igual. Pocos meses después de publicado el estándar se conocieron 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, el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) produjo el adendo IEEE 802.11i [2], donde se especifican los diferentes requerimientos y condiciones necesarias para implementar una red inalámbrica de área local en la que cada usuario tenga una comunicación segura, ya sea con otros usuarios de la red o con un servidor dentro de ésta. Nosotros, en particular, nos preocupamos por el aspecto de la autenticación, dados 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 redes inalámbricas de área local basadas de 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 esta tecnología inalámbrica basada en la infraestructura de un sistema de distribución, y en general a toda red IEEE 802.x.

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 y DIAMETER [3], protocolos de autenticación extensibles (EAP), robustos sistemas de administración de llaves y control de acceso por gestión de puertos; además, se comprobará cómo 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 completo análisis de desempeño en el empleo de los mecanismos, con el fin de describir las generalidades y especificaciones de esta 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. Abordamos finalmente un estudio alrededor de los requerimientos AAA (Autenticación, Autorización y Auditoria)[4] para la prestación de servicios integrales de autenticación, autorización y auditoria en las redes inalámbricas de nueva generación.

En el desarrollo de este documento, la sección II tratará los protocolos de seguridad para la mayoría de las redes inalámbricas implementadas hoy en día, a fin de establecer en la sección III una evaluación de

los requerimientos AAA. En la sección IV se describirá el análisis de desempeño de los protocolos RADIUS y DIAMETER. Finalmente, en las secciones V y VI se describirán los resultados y conclusiones que conllevan a la implementación de uno u otro protocolo.

II. PROTOCOLOS DE SEGURIDAD

A. Protocolo RADIUS

Surgió inicialmente como una solución para la administración en el control de acceso para usuarios que soportaban su conexión mediante enlaces seriales y módems, facilitando el control y supervisión de la seguridad, la autorización, la auditoria, verificación de nombres de usuarios y contraseñas, así como una detallada información de configuración sobre el tipo de servicio que se pretendía entregar al usuario. Los elementos característicos que posee RADIUS [6] le han permitido guardar un alto grado de compatibilidad con la arquitectura dispuesta por las redes inalámbricas IEEE 802.11, una razón primordial por la cual es éste el servidor recomendado, según la norma, para prestar los servicios de autenticación en redes inalámbricas. El protocolo RADIUS sigue un modelo cliente/servidor, donde el papel de servidor es desempeñado por RADIUS, y un elemento de red designado como NAS (Network Access Server), toma la función de cliente de RADIUS; el NAS tiene la responsabilidad de servir como puente o mediador entre los mensajes entrantes y salientes desde y hacia el servidor, es decir, se encarga de retransmitir los solicitudes de conexión, autenticación de usuarios y en general toda la información necesaria para el usuario. Se aclara que el NAS no solicita servicios ni acepta respuestas a los servicios solicitados. En el escenario de una red inalámbrica IEEE 802.11, el punto de acceso toma el papel de NAS. Las transacciones realizadas entre el cliente y el servidor RADIUS son autenticadas mediante la utilización de un secreto compartido, que nunca viajará por la red, además del intercambio entre estos dos puntos de una serie de contraseñas de usuarios, con el fin de minimizar la captura de la contraseña verdadera por parte de algún intruso en la red. En el escenario de una red inalámbrica IEEE 802.11 la administración de llaves, con el fin de garantizar la confidencialidad de los mensajes, se hace mediante un sistema de derivación jerárquico de llaves que autentican la información por cada intercambio de mensaje, dicho sistema se describe en el protocolo IEEE 802.11i.

En cualquier escenario donde se encuentre implementado RADIUS, todo usuario debe presentar ante el cliente o NAS una información de autenticación, dada por un nombre de usuario y una contraseña. Además se requiere de un protocolo de enlace de datos que soporte dentro de sus tramas información de autenticación. Una vez el usuario ha presentado la información de autenticación ante el cliente, éste crea una Solicitud-de-Acceso o Access-Request ante el servidor RADIUS; la solicitud consta, como base, del nombre y contraseña del usuario, de la identificación del cliente y del puerto por el cual el usuario está accediendo. El mensaje de Solicitud-de-Acceso es enviado al servidor RADIUS el cual, tan pronto recibe el mensaje, inicia la validación en primera instancia del cliente; si el servidor no tiene un secreto compartido para la solicitud procedente desde el cliente, el paquete deberá ser silenciosamente descartado. Si por el contrario el cliente es correctamente validado, el servidor RADIUS buscará en una base de datos de usuarios la correspondencia entre el nombre de usuario y la contraseña especificada en la Solicitud-de-Acceso. La base de datos en el servidor contiene adicionalmente una lista de requisitos que deben ser conocidos y especificados inicialmente para permitir el acceso del usuario; por ejemplo en el estándar IEEE 802.11i la configuración de los perfiles de usuarios están considerados de tal forma que el usuario sólo pueda acceder por un puerto específico y a través de un único cliente, mediante la implementación del protocolo IEEE 802.1X

B. Protocolo DIAMETER

Este protocolo surgió, igual que RADIUS, como una solución de autenticación para redes implementadas bajo el protocolo PPP (Point-to-Point Protocol). No obstante, guarda diferencias marcadas que pretenden principalmente brindar extensamente servicios AAA; Dentro de sus facilidades más sobresalientes se encuentra la entrega y manejo de AVPs (Attribute Value Pairs), es decir, unidades de información AAA, unidades para negociación de recursos, unidades para notificaciones de errores, unidades de extensibilidad del protocolo a través de la adición de AVPs y prestación de servicios básicos para aplicaciones, como por ejemplo el manejo de sesiones de usuario. El protocolo lleva a cabo la entrega de información por medio de los AVPs, los cuales son adicionados a los mensajes DIAMETER dependiendo del tipo de solicitud requerida como, por ejemplo, el transporte de la información de autenticación del usuario, con el fin de realizar la búsqueda y verificación de éste en el servidor DIAMETER. Adicionalmente, se considera el transporte de la información de autorización entre clientes y servidores para conceder la solicitud de acceso al usuario y el intercambio de información sobre utilización de recursos, con el fin de desempeñar tareas de auditoria, tales como mantenimiento y gestión de las sesiones, capacidad de los enlaces, registro de errores, etc. Por último, se define la configuración de una jerarquía DIAMETER para llevar a cabo funciones de relevo de servidores para disponibilidad de servicios, resolución de solicitudes descentralizadas y redireccionamiento de mensajes.

El funcionamiento del protocolo DIAMETER cumple con las mismas condiciones que el protocolo RADIUS, en cuanto al número y tipo de mensajes. Sin embargo, sus componentes de red brindan algunas características adicionales que demuestran serias diferencias. En primer lugar, el cliente DIAMETER es, por definición, un dispositivo que se encarga de administrar el control de acceso a un segmento de red específico, basado en el soporte y reconocimiento de las aplicaciones designadas para la red inalámbrica que opera bajo el protocolo DIAMETER; este cliente es el mismo punto de acceso. De igual forma es denominado este dispositivo en el protocolo RADIUS, sin embargo se limita tan sólo a retransmitir las solicitudes y respuestas desde y hacia los extremos de red. Por su parte, el servidor DIAMETER es el dispositivo que se encarga de administrar y atender todas las solicitudes para la autenticación, autorización y auditoria, procedentes desde cualquier usuario en un realm o dominio específico, lo cual ofrece mayores facilidades en la atención de requerimientos originados en redes remotas, mediante la ejecución de agentes, mientras RADIUS prescinde por completo de estas entidades. Por lo tanto es necesario que todo nombre de usuario este separado por el carácter "@" del nombre del dominio, con el fin de determinar si dicha solicitud puede ser atendida localmente o debe ser redireccionada o enrutada. RADIUS también requiere de este formato de nombre de dominio para poner en funcionamiento a sus servidores remotos, aunque la ventaja de DIAMETER es que este parámetro puede ser enviado por piggybacking en el campo para el nombre del DNS, en el mensaje de información sobre la ubicación remota, lo cual contribuye en la disminución del número de paquetes necesarios para el intercambio de datos. Finalmente, los agentes DIAMETER para el redireccionamiento, relevo, Proxy y traducción, se encargan de manera respectiva o conjunta de la distribución de sistemas de administración en grupos para las funciones de asociación segura. Dentro de esta función se encuentran las tareas de concentración de solicitudes desde varios puntos de acceso inalámbricos localizados en la misma área o distribuidos, el procesamiento de valor agregado para ciertas solicitudes o respuestas, la distribución balanceada del tráfico, la organización de las solicitudes hacia las diferentes entidades autenticadoras cuando algunas redes de naturaleza más compleja pueden necesitarlo y mantener un registro salto por salto de las transacciones. Esto se hace con el fin de llevar un completo monitoreo de los eventos y transacciones que

ocurren dentro de la red y bajo el protocolo.

C. Protocolo IEEE 802.1X

El comité técnico del IEEE diseñó un protocolo de acceso al medio por administración de puertos, cuyo funcionamiento es independiente de la norma 802 sobre la cual opera la red. Para las redes inalámbricas de área local el estándar IEEE 802.1X [5] permite hacer interoperable las redes IEEE 802.11 con los protocolos RADIUS y DIAMETER para la prestación de servicios de seguridad. De esta forma, el funcionamiento de uno u otro protocolo se adapta a las condiciones de transacción de 802.1X. El usuario móvil o suplicante y el autenticador o punto de acceso operan sus mecanismos y protocolos de autenticación por medio del PAE (Entidad de Acceso por Puerto). 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. 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 éste a la vez lo envíe hacia el servidor de autenticación, pasando así al estado Authenticating, etapa durante la cual 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 dé la autorización para el acceso del 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 se notificará al usuario que el proceso de autenticación ha fracasado. Finalmente, cuando se quiere terminar con una sesión, el usuario origina una trama EAPOL-Logoff, que pone al suplicante en el estado Logoff y el punto de acceso en Disconnected.

D. Protocolo EAP

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 permitirá 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 Access-Request o Solicitud de Acceso con un atributo de Message-EAP (Mensaje-EAP) [7]. 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 utilizará al autenticador para enviar un paquete Response-EAP (Respuesta-EAP) hacia el servidor y así después de una serie de intercambios opcionales de mensajes de desafíos llegar finalmente a una respuesta de rechazo o aceptación del nodo móvil. Aunque parezca 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 la negociación previa entre el usuario y el autenticador para determinar si en la solicitud, el suplicante es procesable, es decir, si soporta EAP, si puede ser atendida localmente o necesita ser enrutada hacia otro servidor e incluso si el mecanismo de autenticación EAP es aceptado por el usuario. Cualquier desacuerdo en

la negociación del protocolo EAP entre el suplicante, autenticador y servidor arrojará un paquete de Access-Reject o Rechazo-de-Acceso al usuario. La Figura 1 muestra con mayor claridad el proceso descrito. Por otro lado, el punto de acceso puede servir como entidad central de registro para las transacciones realizadas entre diferentes usuarios y servidores de la misma celda.

Figura 1. Mensajes en proceso RADIUS/EAP [8].

La conversación EAP entre el par DIAMETER (suplicante) y el dispositivo de acceso o punto de acceso comienza con la preparación de una solicitud de autenticación EAP del suplicante. Posteriormente, el punto de acceso procede a enviar la solicitud DIAMETER/EAP hacia el servidor compuesta por el nuevo AVP EAP-Payload encapsulando el mismo mensaje de solicitud que en un principio se originó en el par. El servidor atenderá la llegada del paquete con un mensaje de respuesta DIAMETER/EAP que contiene el AVP EAP-Payload con el paquete EAP encapsulado solicitando la identidad al usuario, indicando además en el AVP Result-Code que se esperan solicitudes subsecuentes para finalizar el proceso de autenticación. Una vez el usuario tenga una respuesta para el servidor, éste prepara un paquete EAP de respuesta para el punto de acceso, quien transmitirá una segunda solicitud DIAMETER/EAP hacia el servidor con la identidad del equipo par. El intercambio de paquetes continuará hasta que el servidor tenga un mensaje final de aceptación o rechazo del usuario. Si efectivamente la transacción finaliza con un resultado satisfactorio para el equipo solicitante, el servidor enviará un AVP adicional en su paquete con el material de la llave que protegerá de ahí en adelante la comunicación entre el dispositivo de acceso y el usuario final. En casos particulares donde la solicitud inicial no es de autenticación, sino de autorización el mensaje final del servidor hacia el usuario, será de aceptación condicionada, ya que él necesitará que se envíen adicionalmente los AVPs propios de autorización.

La operación conjunta de este protocolo, junto con el estándar IEEE 802.1X [9] y la recomendación RADIUS o DIAMETER, permiten llevar a cabo los procesos de autenticación de usuarios para obtener las medidas de desempeño y comportamiento dentro del marco de trabajo AAA. En la Figura 2 se ilustra el intercambio de mensajes.

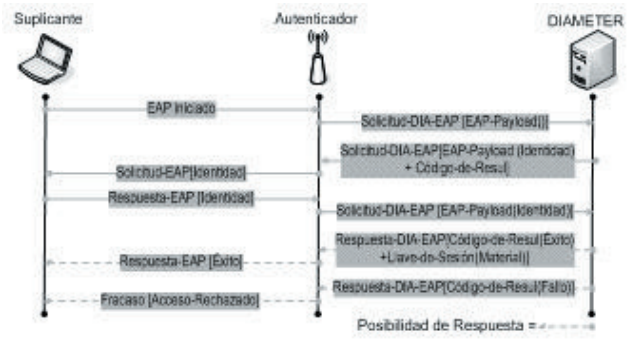

Figura 2. Mensajes en proceso DIAMETER/EAP

III. REQUERIMIENTOS AAA

La evaluación de requerimientos AAA [11] para los protocolos RADIUS y DIAMETER, además del análisis de desempeño de cada uno de ellos se llevó a cabo con base en el escenario de pruebas de la Figura 3, el cual se compone de un servidor RADIUS o DIAMETER, un servidor de certificados para ciertos mecanismos de autenticación, dos puntos de acceso y los clientes o usuarios móviles respectivos. Sobre esta topología se realizaron las medidas y comparaciones de un estándar frente a otro.

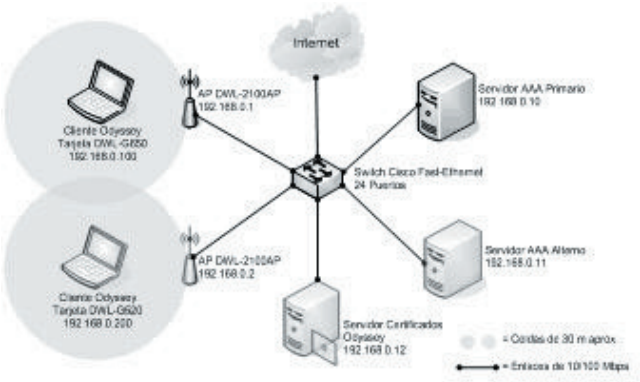

Figura 3. Escenario general de pruebas

Tanto el protocolo RADIUS como el protocolo DIAMETER son denominados protocolos AAA, es decir, que cumplen de forma integral con la prestación de servicios de autenticación, autorización y auditoria. La IETF (Internet Engineering Task Force) en la RFC 3127 establece 25 requerimientos, divididos en 4 categorías: generales, autenticación, autorización y auditoria, los cuales deben ser cubiertos por todo protocolo que pretenda ser amparado por el marco de trabajo AAA. La Tabla 1 ilustra cada uno de los requerimientos, al igual que el desempeño obtenido por cada uno de los protocolos bajo estudio, valorando 3 posibles calificaciones: aprobado (A), en caso de cumplir a cabalidad con el requerimiento; parcial (P), en caso de suplir la necesidad requerida por medio del diseño de herramientas adicionales en las aplicaciones de software o bien sea por el soporte del servicio a través de un protocolo alterno y completamente compatible con RADIUS o DIAMETER; por último la calificación de reprobado (R) se concede cuando el protocolo no tiene herramienta o soporte alguno para el cumplimiento del requerimiento. Las pruebas y procedimientos llevados a cabo para la asignación de las respectivas calificaciones son descritas en el trabajo de grado "Estudio de desempeño en servidores de autenticación RADIUS y DIAMETER para la prestación de servicios de autorización, autenticación y auditoria AAA en redes inalámbricas de área local IEEE 802.11" [10].

Tabla 1. Evaluación de requerimientos AAA de RADIUS y DIAMETER

Requerimiento	RAD	DIA
Escalabilidad	P	A
Detección y recuperación de fallas	R	A
Autenticación mutua	P	A
Seguridad en el nivel de transporte	R	A
Confidencialidad e integridad en los datos	P	A
Transporte de certificados	A	A
Transporte confiable AAA	R	A
Soporte IPv6	A	A
Soporte enrutamiento y Proxy	P	A
No requerimiento de secreto compartido	R	A
Soporte de atributos para servicios	A	A
Soporte de NAI	A	A
Soporte CHAP	A	A
Soporte EAP	A	A
Contraseñas PAP y en texto claro	A	A
Reautenticación por demanda	P	A
Asignación de direcciones dinámicas y estáticas	A	A
Capacidad de rechazo	P	A
Soporte de túneles de capa dos	A	A
Soporte de reglas de acceso y filtros	P	A
Desconexión no solicitada	A	A
Auditoria en tiempo real	A	A
Reporte de auditoria extensible	A	A
Marcas de tiempo de auditoria	A	A
Auditoria dinámica	A	A

Aunque algunas fuentes reconocidas, tales como Cisco Systems, Microsoft Corporation y Funk Software, ubican a RADIUS como un protocolo AAA, el completo análisis de las condiciones que debe reunir para ser considerado como tal, arrojaron una negación definitiva, ya que de los 25 requerimientos AAA, catorce de ellos, que representan el 56% obtuvieron la calificación de aprobado, siete requerimientos, equivalente al 28% son de parcial cumplimiento y los restantes cuatro, igual al 16% fueron reprobados. Sin embargo, resultan evidentes las razones por las cuales se asume que RADIUS puede prestar servicios de autenticación, autorización y auditoria, dado que aquellos requerimientos que se relacionan exclusivamente con estos tres servicios obtuvieron una calificación satisfactoria, variando entre parcial y aprobado.

La mayor deficiencia se observa en los requerimientos generales que de una u otra forma comprometen la confiabilidad, seguridad y disponibilidad del

protocolo, observando con mayor preocupación el requerimiento de la escalabilidad, el cual demuestra una significativa limitación en el soporte de un número importante de usuarios, restringiendo de este modo el uso del protocolo RADIUS a entornos con bajas densidades de clientes finales, ya que por un lado los puntos de acceso en los ambientes inalámbricos estudiados soportan hasta 2048 nodos asociados, pero RADIUS sólo puede solucionar las peticiones de acceso de un máximo de 255, desperdiciando una eficiencia inherente de la tecnología inalámbrica de área local IEEE 802.11. Otro de los requerimientos para el que no se ha ideado solución alguna es la detección de fallas, lo cual en primer lugar no permite al usuario conocer las verdaderas razones para que su solicitud no haya sido resuelta exitosamente y en segundo lugar la caída del sistema de prestación de servicios, en caso de no poseer enlaces redundantes y servidores secundarios de respaldo. Los dos últimos requerimientos reprobados fueron la seguridad en el nivel de transporte y el transporte seguro AAA, que confirma las profundas vulnerabilidades de RADIUS para ser aceptado con todo mérito en el grupo de protocolos AAA. Por su parte DIAMETER obtuvo un 100% de aprobados en la evaluación de requerimientos, validando el propósito y la motivación para el diseño de este protocolo, el cual fue concebido bajo lineamientos AAA ya homologados, junto con una plataforma adaptable a casi cualquier red de comunicación de datos de la actualidad, ya que ofrece todas las garantías necesarias para la prestación de servicios de autenticación, autorización y auditoria.

IV. ANÁLISIS DE DESEMPEÑO DE PROTOCOLOS DE SEGURIDAD

Determinar la conveniencia de la utilización del protocolo RADIUS o DIAMETER para los servicios de autenticación, autorización o auditoria en una red inalámbrica IEEE 802.11, responde no sólo al cumplimiento de los parámetros AAA, sino también al desempeño demostrado desde el inicio hasta la finalización de aquellos procesos de mayor relevancia para el usuario. Para el análisis de desempeño desarrollado, se tomaron los procesos de autenticación con diversos mecanismos y la utilización de agentes de enrutamiento y proxies, como las pruebas a partir de las cuales, se podrán establecer las conclusiones necesarias para conocer cuál de los dos presuntos protocolos AAA, resulta ser más apto para la prestación de los servicios de seguridad de una red inalámbrica.

A. Protocolo RADIUS

El desempeño del protocolo RADIUS se mide de acuerdo con el comportamiento demostrado en la autenticación de usuarios mediante los mecanismos EAP-TTLS (Tunneled Transport Layer Security) [12] y PEAP (Protected EAP), con algoritmos internos de cifrado PAP (Password Authentication Protocol), MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol) y EAP-MS-CHAPv2, para que finalmente con estadísticas tales como la media, el coeficiente de variación y la desviación estándar, se establezcan las fortalezas y debilidades internas en el comportamiento del protocolo, al igual que las ventajas y desventajas comparativas de uno contra otro. Los mecanismos de autenticación analizados son en primer lugar EAP-TTLS con algoritmo interno de cifrado PAP y posteriormente con MS-CHAPv2, los cuales son versiones populares y de uso más generalizado para el intercambio de credenciales. El segundo mecanismo es PEAP con algoritmo interno de cifrado EAP-MS-CHAPv2, el cual es el único mecanismo de autenticación dispuesto para plataformas Windows XP Service Pack 2.

Durante la autenticación EAP-TTLS con PAP, el primer paquete Access-Request transporta en el atributo EAP-Message la identidad del equipo móvil, es decir, el nombre de usuario; no obstante para la autenticación EAP-TTLS es posible ocultar el nombre verdadero con un nombre falso programado por el cliente, de tal forma que el analizador de protocolo mostrará el nombre falso de usuario en el atributo User-Name.

Si el nombre es verificado satisfactoriamente en el servidor, éste enviará un paquete Access-Challenge definiendo el mecanismo que propone para la autenticación del usuario, en este caso TTLS. Si el mecanismo es soportado por el cliente, se iniciará con el nuevo mensaje Access-Request la sesión SSL (Secure Socket Layer) implementando el protocolo TLS, enviando internamente el paquete de saludo al cliente (Hello Client) con las llaves de cifrado y métodos de compresión. El servidor en respuesta enviará su certificado digital que permite al cliente verificar si es un servidor de confianza, junto con el certificado viaja la llave pública para la encripción de los mensajes siguientes. El cliente con el envío de un Access-Request confirma la instalación de la llave pública en su equipo local, para que a continuación el servidor prepare un desafío encriptado con la llave ya presente en ambos extremos, validando de esta manera si la llave fue propiamente instalada en el cliente; de ser así éste se dispondrá a transmitir su llave pública de cifrado hacia el servidor, quien confirmará su instalación con el envío de un mensaje encriptado. Si el mensaje es correcto, el usuario responde con un mensaje de aplicación que finaliza el establecimiento del túnel virtual en el canal de comunicación y el servidor podrá emitir finalmente su mensaje Access-Accept con las llaves de encripción de datos, derivadas de la contraseña PAP y almacenadas en los atributos Vendor-Specific.

En la autenticación EAP- TTLS con MS-CHAPv2 se necesita intercambiar doce mensajes entre el servidor y el usuario para llevar a cabo de forma satisfactoria el proceso de autenticación, desde la primera solicitud de acceso hasta la respuesta de aceptación. El método de cifrado interno hereda el funcionamiento del tradicional CHAP del protocolo PPP (Point-to-Point Protocol) con una secuencia binaria de 16 bytes, generada a partir de la contraseña de usuario y los campos propios del paquete RADIUS; sin embargo Microsoft, quien posee la patente de este método, reforzó la generación de los datos cifrados con un módulo muy similar al trabajado por el método MD5 (Message Digest 5). Adicionalmente, la razón por la cual se necesita de dos paquetes más para completar la autenticación, es la utilización de dos llaves CHAP para ser instaladas en el equipo cliente de tal forma que al paquete con el mensaje de aplicación enviado por el cliente, el servidor responda con uno igual, pero utilizando la segunda llave CHAP. Si el mensaje es correctamente verificado por el usuario, el servidor enviará un paquete Access-Request confirmando que el intercambio de las herramientas de cifrado funcionan correctamente; en este momento el servidor está listo para emitir su mensaje de aceptación.

El mecanismo PEAP es un desarrollo de Microsoft, por lo tanto sólo es compatible con plataformas de este tipo, incluso las opciones disponibles para algoritmos internos de cifrado son escasas, la primera de ellas es EAP-MS-CHAPv2 y la segunda es EAP-GTC (EAP Generis Tocken Card) que sólo funciona con equipos inalámbricos de la compañía Cisco Systems. Este mecanismo de autenticación intercambia una totalidad de veinte mensajes antes de completar el proceso de autorización para el acceso del usuario, donde las doce primeras transacciones cumplen los mismos objetivos de la autenticación EAP-TTLS con MSCHAPv2, es decir, el intercambio del certificado digital del servidor, las credenciales del usuario y las llaves derivadas del algoritmo de cifrado; los paquetes adicionales son mensajes de aplicación que comprueban mediante desafío y respuesta la instalación de llaves MS-CHAP, tanto en el equipo servidor como en la estación del cliente.

B. Protocolo DIAMETER

Actualmente, el protocolo DIAMETER no posee un desarrollo comercial muy avanzado, dada su novedad y el trabajo implícito que involucraría la transacción de servicios soportados por el protocolo RADIUS en redes de corto o amplio cubrimiento. Debido a esto muchas de las pruebas realizadas no pueden ser analizadas desde un punto de vista comparativo, ya

que el paquete cliente/servidor DIAMETER disponible actualmente es un proyecto de código abierto, conocido como OpenDiameter, el cual a pesar de llevar una evolución ciertamente avanzada, son varias las deficiencias que aún guarda, como por ejemplo la ausencia de agentes Proxy, agentes de relevo, agentes de redireccionamiento, agentes de traducción y aplicaciones de movilidad.

El mecanismo EAP-TTLS se aplica de la misma forma para el protocolo DIAMETER, la docena de mensajes intercambiados llevan a cabo una transacción idéntica en el reconocimiento de certificados y credenciales, pero con la diferencia de emplear como algoritmo interno de cifrado al mecanismo EAP-MD5, ya que la aplicación OpenDiameter utilizada, pertenece a un proyecto de arquitectura abierta, que reemplaza el método MS-CHAPv2 de Microsoft con MD5. Además los atributos intercambiados de cada paquete DIAMETER evidentemente son diferentes para cada mensaje, llevando a encontrar las mayores diferencias en los valores de cabecera de AVPs y datos efectivos. Finalmente, en el segundo de los mecanismos de autenticación implementados, el esquema PEAP con EAP-MD5 como algoritmo interno de cifrado para el envío de las credenciales de usuario, los mensajes intercambiados entre el usuario y el servidor son veinte en total, con un funcionamiento idéntico al descrito en el protocolo RADIUS.

V. RESULTADOS

El cálculo de la media en la Figura 4 establece inicialmente que los tiempos de respuesta promedio que toma realizar una autenticación de usuario con el protocolo RADIUS y DIAMETER es prácticamente el mismo, independientemente del mecanismo de autenticación usado, aunque para los dos protocolos resulta ligeramente más ágil un procedimiento de autenticación EAP-TTLS con MS-CHAPv2 para plataformas Windows, y EAP-MD5 como algoritmo interno de cifrado para plataformas libres, como por ejemplo Linux o FreeBSD.

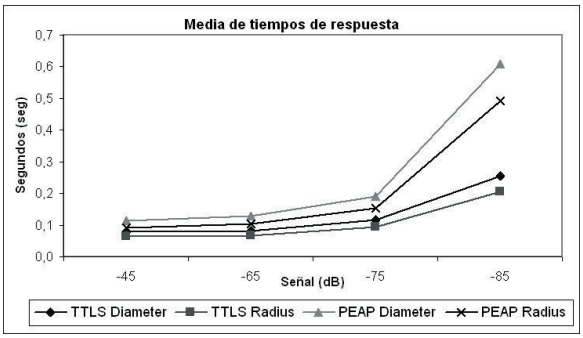

Figura 4. Media de tiempos de respuesta

La media de parámetros de desempeño de la Figura 5 demuestra que al emplear mecanismos de autenticación, tales como EAP-TTLS y PEAP el tráfico que deberá generar el servidor será mayor al tráfico recibido, debido al intercambio unilateral del certificado digital de reconocimiento ante el usuario; pero si se habilita la opción de autenticación a través de certificados digitales en el usuario, la proporción de bytes de tráfico se equilibraría a niveles semejantes al de tráfico recibido. Las cabeceras de atributos y AVPs ocupan en cualquiera de los casos una proporción menor de la capacidad del canal de comunicación con respecto a la cantidad total de información efectiva. Sin embargo, las cabeceras de AVPs DIAMETER son tres veces más grandes que las cabeceras de atributos RADIUS, ya que el campo de código pasa de tener 8 bits a 32 bits, además de los bits de banderas, que permiten una implementación muy extensa de AVPs (17 millones), además de incluir servicios de seguridad exclusiva por cada AVP; lo cual puede entenderse como un sacrificio aceptable en la relación costo-beneficio.

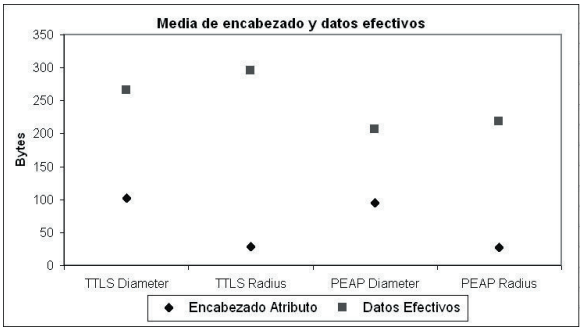

Figura 5. Media de parámetros de desempeño

El coeficiente de variación de los datos efectivos de la Figura 6 demuestran que los valores más altos son para el mecanismo de autenticación EAP-TTLS con el protocolo DIAMETER, aunque los demás valores para el mecanismo EAP-TTLS y PEAP con RADIUS, registra también cifras elevadas, debido a la diversidad de tamaño en los paquetes, encontrando de forma sistemática mensajes cortos en los paquetes Access-Request desde el usuario y mensajes muy largos en los paquetes Access-Challenge desde el servidor, donde es indiferente si se implementa el protocolo DIAMETER o RADIUS.

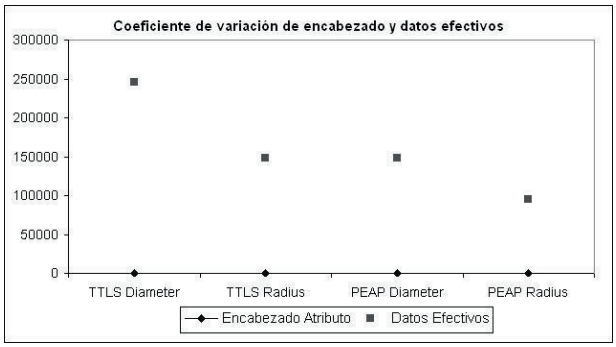

Figura 6. Coeficiente de variación de parámetros de desempeño

La razón para que no existan diferencias significativas en el desempeño de un protocolo frente a otro, se debe a que los dos soportan su servicio de autenticación en el protocolo EAP, el cual trabaja de igual manera, si se tienen procesos de encapsulamiento RADIUS o DIAMETER, es decir la cantidad y la naturaleza de las transacciones serán siempre las mismas. Adicionalmente, el protocolo DIAMETER como sucesor de RADIUS fue diseñado para ofrecer mayores facilidades para la instalación y soporte de nuevos servicios, lo cual fue conseguido por completo, con prácticamente los mismos parámetros de desempeño.

Tras el análisis teórico de las recomendaciones de los protocolos RADIUS y DIAMETER, la evaluación de requerimientos AAA y el análisis de desempeño con diferentes mecanismos de autenticación se puede asegurar que el protocolo que demuestra una ventaja sobresaliente en cada uno de estos aspectos es DIAMETER, siendo así el protocolo de mayor conveniencia para el soporte de servicios AAA en redes inalámbricas de área local IEEE 802.11. Sin embargo, en términos prácticos de implementación el protocolo RADIUS posee un mayor reconocimiento y popularidad frente al protocolo DIAMETER, ya que éste último posee un desarrollo muy reciente y por ende las herramientas dispuestas en las pocas aplicaciones disponibles son limitadas, las cuales por el momento no sobrepasan más que un ejercicio académico de algunas universidades. De acuerdo con esto, muchos de los retos pendientes por abordar se centran en el desarrollo de librerías y aplicaciones para el soporte de movilidad y agentes de traducción para DIAMETER.

REFERENCIAS

[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] CHEN, J.C. JIANG, M.C. y LIU, Y. "Wireless LAN Security and IEEE 802.11i", Wireless Communications Magazine, Febrero 2005, pp. 27 – 36.

[4] BARI , F. y BOUTHEMY, J.L. "An AAA based service customization framework for public WLANs", Wireless Communications and Networking Conference 2005, Marzo 2005, pp. 2430 – 2435.

[5] HECKER, B. y LABOID, H. "Pre-authenticated signalling in wireless LANs using 802.1X access control", Global Telecommunications Conference, 2004. GLOBECOM '04, Noviembre 2004, pp. 2180 -2184.

[6] RIGNEY, C. WILLENS, S. RUBENS, A. y SIMPSON, W. "Remote Authentication Dial In User Service (RADIUS)". IETF RFC 2865, Junio 2000.

[7] ABOBA, B. BLUNK, L. VOLLBRECHT, J. CARLSON, J. y LEVKOWETZ, H. "Extensible Authentication Protocol". IETF RFC 3748, Junio de 2004.

[8] ABOBA, B. y CALHOUN, P. "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)". IETF RFC 3579, Septiembre 2003.

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

[10] CHAPARRO, R. "Estudio de desempeño en servidores de autenticación RADIUS y DIAMETER para la prestación de servicios de autorización, autenticación y auditoria AAA en redes inalámbricas de área local IEEE 802.11" Trabajo final de grado. Universidad Militar Nueva Granada, Bogotá – Colombia, Julio 2006.

[11] MITTON, D. ST. JOHNS, M. BARKLEY, S. NELSON, D. PATIL, B. STEVENS, M. y WOLF, B. "Authentication, Authorization and Accounting: Protocol Evaluation", IETF RFC 3127, Junio de 2001.

[12] FUNK, P. y BLAKE-WILSON, S. "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)," IETF Internet draft, Agosto 2003, trabajo en progreso.

BIOGRAFÍAS

Marcela Mejía Fajardo - Nació en Bogotá, Colombia. Es ingeniera electrónica de la Universidad Santo Tomás de Bogotá, Colombia. Obtuvo su título de Maestría en Teleinformática de la Universidad Distrital Francisco José de Caldas de Bogotá, Colombia. Actualmente se encuentra adelantanado sus estudios de doctorado en el área de seguridad informática sobre redes inalámbricas en la Universidad de los Andes, Colombia, y pertenece al grupo WiNET, donde se realizan estudios sobre redes inalámbricas.

Ramiro A Chaparro Vargas - Nació en Cúcuta, Colombia. Es egresado del programa de ingeniería en telecomunicaciones de la Universidad Militar Nueva Granada. Actualmente se encuentra desempeñando labores como ingeniero en el sector empresarial y se mantiene vinculado con el grupo de investigación WiNET.