Análisis del desempeño del protocolo RADIUS en redes inalámbricas

Alejandra Mendoza Carreón, Alejandro Barraza Herrera, Fernando Estrada Saldaña, Cynthia Esquivel Rivera, Daniela Calderón Navarro

Universidad Autónoma de Ciudad Juárez

RESUMEN

Las redes inalámbricas se han vuelto el método más utilizado para conectarse a Internet. Por la naturaleza vulnerable de este tipo de comunicación, se han diseñado protocolos de seguridad que permite la transmisión confiable de información a través de este medio inseguro. Sin embargo, la implementación de protocolos de seguridad puede ocasionar que el rendimiento de las redes inalámbricas baje, al consumir recursos de los dispositivos y ancho de banda extra para su correcto funcionamiento. En este documento se analiza el desempeño del protocolo RADIUS al ser implementado en una red inalámbrica.

Palabras clave: Redes inalámbricas, Protocolo RADIUS, Transmisión de datos.

INTRODUCCIÓN

Debido al notable incremento en la demanda de conexiones de redes inalámbricas a Internet, cada vez es son más las compañías que ofrecen sus servicios de conexión públicos haciendo común el encontrar puntos de acceso inalámbricos en diferentes establecimientos comerciales.

Las redes inalámbricas son por naturaleza, vulnerables a ataques. Por esto surgen los protocolos de seguridad que permiten desde la restricción del acceso a la red, hasta opciones avanzadas de seguridad. Varios protocolos de seguridad han sido diseñados a lo largo de la existencia de las redes inalámbricas, y aunque algunos han sido catalogados como no seguros, se siguen utilizando para implementar medidas mínimas de seguridad. A la medida que los protocolos han sido quebrantados por los llamados piratas cibernéticos, se han diseñado protocolos mas robustos que permiten asegurar la información en su recorrido por las redes inalámbricas. Sin embargo, entre más robusto sea un protocolo de seguridad, mayor será su impacto en el desempeño de la red. Tal es el caso del protocolo RADIUS (*Remote Authentication Dial in User Service*), que se usa principalmente en implementaciones de redes inalámbricas empresariales y provee servicios de autenticación, autorización y contabilidad. En este documento se analiza el desempeño del protocolo RADIUS, implementado en una red inalámbrica en la cual se han implementado otros protocolos de seguridad. El desempeño se midió en tiempo de conexión, autenticación y transferencia.

IMPLEMENTACIÓN

Para el análisis del desempeño de los diferentes protocolos, se implementó una red inalámbrica en un laboratorio. Se utilizaron

6 computadoras, 5 como clientes inalámbricos y una como servidor para la implementación de RADIUS. Además se utilizó el ruteador Linksys modelo WRT54G con un *firmware* versión 1.02.8 que soporta los estándares 802.11b y g, el cual funge como un punto de acceso inalámbrico que sirve como punto intermedio entre los clientes y el servidor RADIUS. La figura 1 muestra la topología implementada.

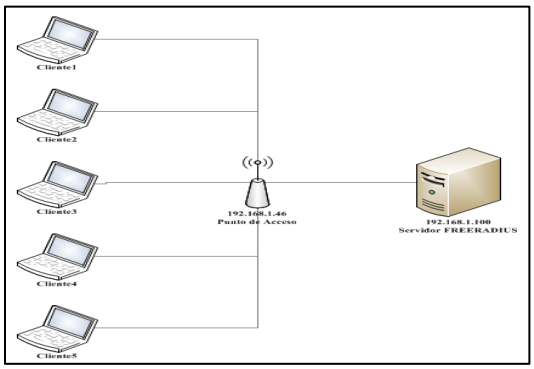

Fig. 1. Topología de red.

Para la implementación de la red, fue necesario utilizar software especializado para el funcionamiento de la red, y la captura de paquetes para el análisis del desempeño. El software que se utilizó fue el siguiente: SQL Server 2005, TekRADIUS, FreeRadius, Golden FTP server y Wireshark.

Cada computadora fue configurada con la información IP necesaria para su conexión a la red, y el punto de acceso fue configurando con distintos protocolos de seguridad para registrar su desempeño. Los protocolos de seguridad implementados fueron WEP (*Wired Equivalent Privacy), y* WPA 2 (*Wi-Fi Protected Access II*), cada uno con diferentes variaciones de implementación. El protocolo WEP se configuró tanto para 64 bits como para 128, y WPA2 se implementó con AES (*Advanced Encryption Standar*) y TKIP (*Temporary Key Integrity Protocol*) +AES.

Después de la implementación de cada protocolo, se procedió a generar tráfico entre las diferentes computadoras y éste fue capturado por el analizador de paquetes Wireshark. Los paquetes filtrados para calcular los tiempo fueron de los protocolos TCP (*Transmisión Control Protocol*), DHCP (*Dynamic Host Configuration Protocol*), y EAPOL/EAP (*Extensive Authentication Protocolo ver LAN*). La figura 2 muestra el filtrado de paquetes en el analizador.

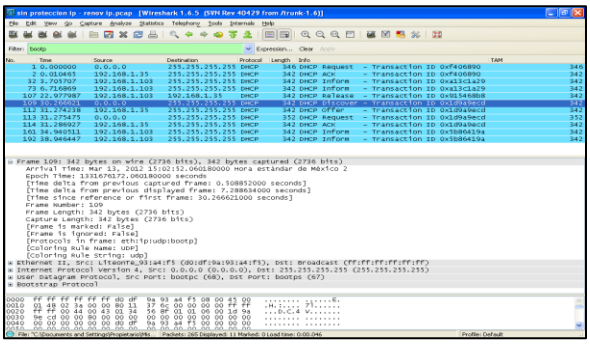

Fig. 2. Filtrado de paquetes en Wireshark.

RESULTADOS.

A continuación se presentan los resultados de la comparación del desempeño del protocolo RADIUS con la implementación de diferentes protocolos de seguridad inalámbricos.

Tiempo de autenticación a la red.

Para calcular el tiempo de autenticación fue necesario capturar paquetes del protocolo EAPOL/EAP tomando en cuenta la diferencia de tiempo entre el momento en que se envió la petición y el momento en que se recibe la respuesta a

dicha petición, los resultados obtenidos se pueden ver en la figura 3.

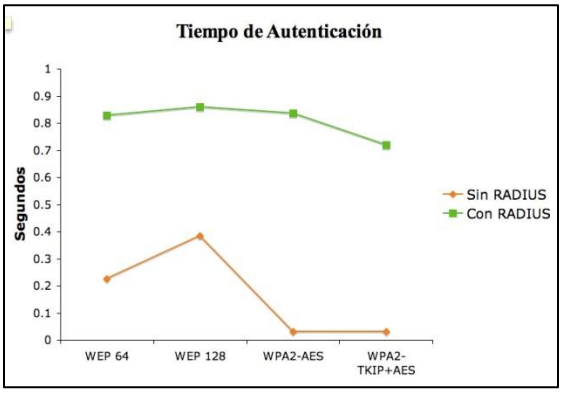

Fig. 3. Tiempo de autenticación.

En la gráfica se observa que al implementar algún protocolo de seguridad como lo son WEP y WPA con sus respectivos tipos de cifrado no les toma más de 0.4 segundos en poder ser autentificados a la red ya que solamente están bajo sus propios parámetros de seguridad, mientras que al implementarse estos protocolos de seguridad en conjunto con RADIUS el tiempo de autenticación se eleva alrededor de 0.6 segundos en promedio, que representa hasta cuatro veces el tiempo de autenticación sin incluir RADIUS. Lo anterior debido a que se tiene que tomar en cuenta el tiempo que tarda el punto de acceso en mandar la petición del cliente al servidor RADIUS para que éste pueda verificar las credenciales del cliente.

Tiempos de conexión a la red.

Para calcular el tiempo de respuesta de obtención de dirección IP, fue indispensable la captura de paquetes DHCP, tomando en cuenta la diferencia desde que el cliente solicita conexión al punto de acceso y éste le asigne la dirección IP que le corresponda, los resultados obtenidos se muestran en las siguientes gráficas donde se puede observar los tiempos que tardó cada cliente en obtener una dirección IP y se muestra los tiempos de conexión bajo el servidor de autenticación RADIUS.

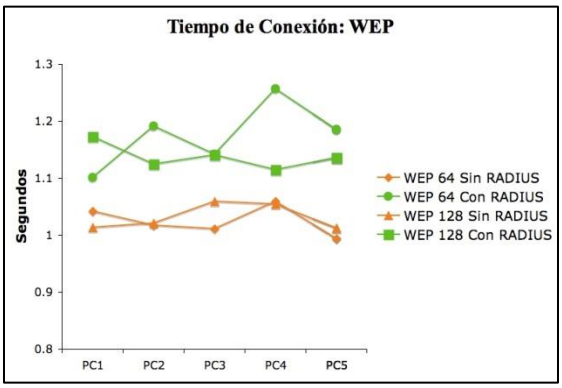

Fig. 4. Tiempos de conexión WEP.

En la figura 4, se muestra que el tiempo que tardó cada una de las computadoras en obtener una dirección IP usando el protocolo WEP de 64 y 128 bits, aquí se observa que siempre que se usa RADIUS, el tiempo que toma la conexión es mayor, hasta en un 15%.

En la figura 5 se observa un comportamiento similar usando el protocolo WPA2. Usando RADIUS, el tiempo de conexión incrementa en promedio 10% para AES y un 14%para AES+TKIP.

Tiempo de transferencia de archivos.

Otras de las pruebas que fueron realizadas en la red que se implementó fue la transferencia de archivos, esto con la ayuda de un servidor FTP, y bajo los mismos parámetros de los protocolos de seguridad implementados. El tiempo se obtuvo en base a los segmentos TCP, tomando la diferencia entre la primera bandera SYN que indica el inicio del envío del archivo hasta la

bandera FIN que indique el final de la transferencia.

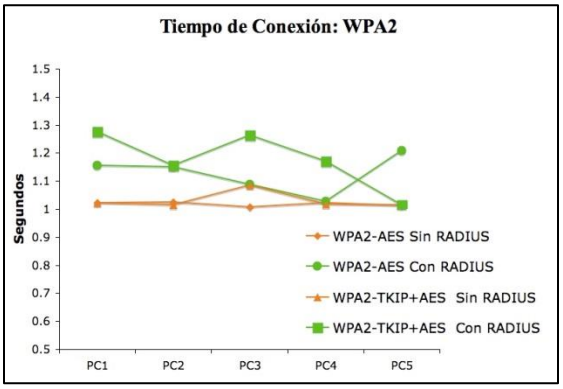

Fig. 5. Tiempos de conexión WPA2.

La figura 6 muestra el tiempo de transferencia de un archivo de 500 KB Utilizando WEP, aquí se observa que toma más tiempo hacer la transferencia del archivo si se implementa RADIUS para WEP 64, hasta en un 63% más en promedio. Sin embargo para WEP 128 toma un 2% menos de tiempo en promedio, para hacer la transferencia con RADIUS.

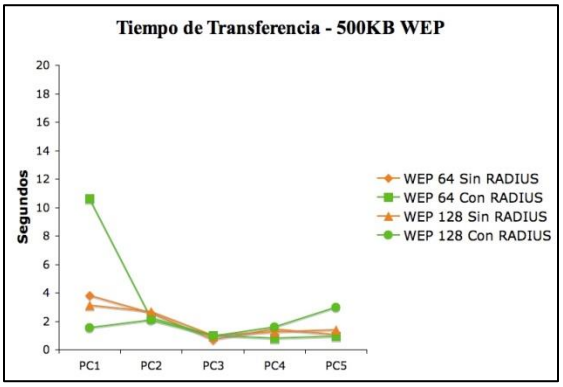

Fig. 6. Tiempo de transferencia (500KB) WEP.

La figura 7 muestra el tiempo que tarda en transferirse el archivo utilizando WPA2, y se puede observar que la transmisión a través de WPA2 AES tarda en promedio 3.5% menos implementando RADIUS, y para WPA2 TKIP+AES el tiempo incrementa un 33% promedio, si se utiliza RADIUS en el sistema. El impacto que tiene RADIUS en la transferencia no es tan significativo, en especial si no se activan los servicios de contabilidad.

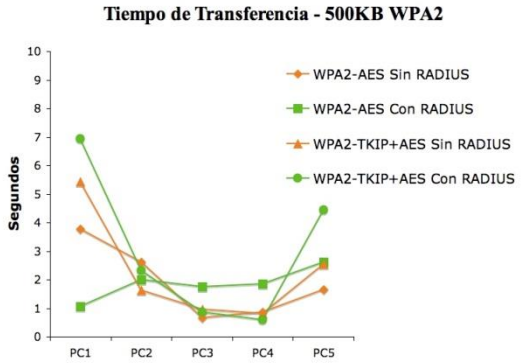

Fig. 7. Tiempo de transferencia (500KB) WPA2.

CONCLUSIONES

Se ha implemnetado una red de prueba inalámbrica para probar el funcionamiento del protocolo RADIUS al implemnetarlo como opción complementaria de seguridad a los protocolos WEP y WPA2.

Los resultados muestran que en general, si se agrega RADIUS el tiempo que tarda la autenticación y conexión de equipos, así como el tiempo de transferencia de archivos, incrementa en ocasiones hasta en un 63% promedio.

El uso de protocolos de seguridad en redes inalámbricas es necesario para la protección de información, sin embargo se debe tener en consideración, que entre más robusto sea un protocolo de seguridad, mayor será su impacto en el desempeño de

una red, siendo esto un factor importante en las decisiones de configuración de la misma.

REFERENCIAS

Borse, M., Shinde, H., (2005), Wireless Security & Privacy. IEEE International Conference on Personal Wireless Comunications.

Chamorro, J.M. (2005), "Consideraciones para la implementación de 802.1x en WLAN´s", SANS Institute Reading Room site., Bogota, Colombia, GIAC Security Essentials Certification Practical Assignment Version 1.4c.

Jagetia, M., Kocak, T.A. (2004), Novel Scrambling Algorithm for a Robust WEP Implementation. IEEE Vehicular Technology Conference, Volumen: 5.

Jordán Calero, J., Huidrobo, J.M., Blanco, A. (2006), Redes de área local: administración de sistemas informáticos, 2da ed. Paraninfo: Madrid, España.

Microsoft., Protocolo de autenticación extensible (EAP), [En Línea], Microsoft Tech Net. Disponible en: technet.microsoft.com/es-es/library/cc782159(WS.10).aspx, Recuperado el 6 de Diciembre del 2012

R. Molva, D. Samfat, and G. Tsudik (1994), "Authentication of mobile users," IEEE Network, vol. 8, no. 2, pp. 26–34.

Muñoz Villa, D.G., (2006). Seguridad en redes WLAN. (Tesis de Licenciatura – Universidad Politécnica Salesiana Ecuador), [En Línea]. Disponible en: http://dspace.ups.edu.ec/handle/123456789/217?mode=full&submit_simple=Muestra+el+registro+Dublin+Core+complemento+del+%C3%ADtem, Recuperado el 5 de Diciembre del 2012.

Pellejero, I. (2006), "Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica", Redes WLAN: Aspectos básicos, Marcombo, Barcelona, España.

Tanenbaum, A. S. (2003), Redes de Computadoras, 4ta ed. México D.F.: Pearson Education.

Whiting, D., Housley, R. (2003), Counter with CBC-MAC (CCM), [En Línea]. Disponible en: www.ietf.org/rfc/rfc3610.txt, Recuperado el 22 de Diciembre del 2012.