17

Fecha de presentación: septiembre, 2016
Fecha de aceptación: noviembre, 2016
Fecha de publicación: Diciembre, 2016

PROPUESTA DE PROTOCOLOS

DE SEGURIDAD PARA LA RED INALÁMBRICA LOCAL DE LA UNIVERSIDAD DE CIENFUEGOS

PROPOSAL OF SECURITY PROTOCOLS FOR THE LOCAL WIRELESS NETWORK OF THE CIENFUEGOS UNIVERSITY

Ing. Alex González Paz[1]
E-mail: agpaz@ucf.edu.cu
MSc. David Beltrán Casanova[2]
E-mail: dbeltranc@uclv.edu.cu
Dr. C. Ernesto Roberto Fuentes Gari[1]
E-mail: gari@ucf.edu.cu
[1]Universidad de Cienfuegos. Cuba.
[2]Universidad Central "Marta Abreu" de Las Villas. Cuba.

¿Cómo referenciar este artículo?

González Paz, A., Beltrán Casanova, D., & Fuentes Gari, E. R. (2016). Propuesta de Protocolos de Seguridad para la Red Inalámbrica Local de la Universidad de Cienfuegos. Universidad y Sociedad [seriada en línea], 8 (4), pp. 128-135. Recuperado de http://rus.ucf.edu.cu/

RESUMEN

En este trabajo se caracterizan las posibles amenazas en redes inalámbricas, los protocolos de seguridad creados para las redes WLAN como: WEP, 802.11i, WPA y WPA2, y protocolos aplicados a otros tipos de redes como las redes LAN cableadas que pueden ser aplicados en redes WLAN. Se realiza un análisis comparativo de los mismos basado fundamentalmente en cuanto al método de autenticación y la técnica de cifrado. Se concluye con la selección de los protocolos de seguridad para la red WLAN de la Universidad de Cienfuegos.

Palabras clave: Protocolos de seguridad, método de autenticación, Radius, técnica de cifrado, WEP, WLAN, WPA, WPA2.

ABSTRACT

In this paper there is a characterization of the potential threats in wireless networks, the safety protocols created for the WLAN such as: WEP, 802.11i, WPA and WPA2, and protocols applied to others types of networks like the LAN networks wired which can be applied in WLAN networks. There is a comparative analysis of the safety protocols based mainly in the authentication method and the encryption technique. It concludes with the selection of the safety protocols for the WLAN of the Cienfuegos University.

Keywords: Authentication Method, Radius, safety protocols, Encryption technique, WEP, WLAN, WPA, WPA2.

INTRODUCCIÓN

En la actualidad las redes inalámbricas de área local, de sus siglas en inglés Wireless Local Area Network (WLAN) han encontrado una variedad de escenarios de aplicación, tanto en el ámbito residencial como en entornos empresariales, por las ventajas que poseen en cuanto a la movilidad, facilidad de instalación y flexibilidad ya que permiten llegar a zonas donde no es posible el cableado o este resulta más costoso. Es por ello, que las empresas analizan la viabilidad de realizar un proceso de actualización de sus redes e introducen redes inalámbricas como complemento de las redes cableadas.

Sin embargo, en su implementación, la seguridad es un aspecto importante ya que a diferencia de las redes cableadas no es necesaria una conexión física. En una red WLAN el medio de transmisión es el aire y los datos son transmitidos mediante ondas de radio que se propagan entre clientes inalámbricos y puntos de acceso (AP). Las ondas de radio atraviesan objetos como techos, pisos y paredes, y los datos transmitidos pueden llegar a destinatarios no deseados. De esta manera, terceros tienen la posibilidad de acceder a dicha información.

En las universidades, además del riesgo de sufrir ataques desde fuera de su perímetro, se ofrecen servicios a distintos tipos de clientes: usuarios administrativos, no docentes, y usuarios del ámbito académico, compuestos por profesores, investigadores y estudiantes, algunos de los cuales pueden ser personas con conocimientos sobre cómo vulnerar la seguridad de la red. En este sentido, resulta imprescindible disponer de políticas de seguridad para este tipo de entorno, de manera que permitan garantizar a un nivel aceptable, la autenticidad, disponibilidad y confidencialidad de la información que se genera y se transmite y con ello el funcionamiento de la red.

En la Universidad de Cienfuegos (UCF) se está trabajando para ampliar los servicios de red WLAN por las ventajas que proveen a los usuarios, además para que los servicios de red lleguen a algunos puntos críticos de la universidad en los que no puede llegar el cableado ya sea por las condiciones del lugar o por los costos que implica, y donde radican o se reúnen estudiantes y profesores con dispositivos que permiten conexión inalámbrica. Para ello se cuenta con el diseño de la red WLAN de la UCF donde se establecen las ubicaciones de los AP. Pero no se han implementado protocolos de seguridad y control de acceso que garanticen que se conecten solo las personas autorizadas y la confidencialidad de la información transmitida.

Al principio se implementó el método de autenticación abierta (sin clave), en el que al operar en este modo un AP, acepta cualquier solicitud. Después se logró configurar una variante en la cual el AP posee una lista de direcciones MAC autorizadas, pero esta implica un esfuerzo adicional a la administración de la red, pues se deben mantener actualizadas las listas de direcciones MAC en cada AP. Luego fue implementado WEP con una clave compartida, pero un inconveniente de este proceso es que las claves WEP tienen vulnerabilidades que son utilizadas para cifrar y descifrar los datos transmitidos. Por lo que los intrusos pueden acceder a herramientas que permiten descifrar las claves, como AirCrack.

En su momento se utilizó WPA con clave compartida, el cual funcionó satisfactoriamente, pero dependía de la clave solamente para acceder a la red y si un usuario autorizado a acceder a la red les proporcionaba la clave a otros sin permisos de acceso, estos podían acceder sin autorización. Por otra parte, si se extravía un dispositivo con la clave almacenada, la misma queda comprometida y se volvió al método de autentificación abierta con una lista de direcciones MAC autorizadas.

Es de interés para la administración de la red de la UCF tener almacenados los registros de conexión de los usuarios para ver los servicios solicitados, lo cual ayuda a la toma de decisiones y permite auditarlos en un momento dado, pero para ello es necesario que los mismos sean autentificados con sus credenciales, lo que no se ha logrado hasta el momento.

Por todo lo anteriormente descrito es necesario implementar protocolos de seguridad en la red WLAN de la UCF que permitan garantizar a un nivel aceptable la autenticidad, disponibilidad y confidencialidad de la información que se genera y se transmite y además permitir autentificar a los usuarios en la red mediante sus credenciales.

Teniendo en cuenta lo analizado se considera como problema científico a resolver en este trabajo, la no existencia de protocolos de seguridad y control de acceso en la red WLAN de la UCF que permitan hacerles frente a las amenazas y ataques que pueda afrontar. Se caracterizan los protocolos de seguridad en redes WLAN, se realiza un estudio comparativo de los mismos con la selección de los que formarán parte de la propuesta para la red WLAN de la UCF.

El estudio comparativo es realizado teniendo en cuenta la evolución de los protocolos que se llevó a cabo después de la descripción de cada uno y con respecto a los anteriores. Se emplearon materiales bibliográficos referidos a la temática sobre posibles ataques, el estándar 802.11i, mecanismos de control de acceso, bibliografía de fabricantes de equipamiento WLAN como Cisco y NETGEAR. Además, se hace una revisión de las RFC para Radius.

A partir de la recolección de información se realiza una valoración para determinar cómo ocurre el proceso de autentificación y conexión, cuáles son las vulnerabilidades asociadas, los principales elementos en los que se debe trabajar y la necesidad de emplear mecanismos de seguridad en redes WLAN. Para comparar los protocolos de seguridad se analizó un AP de prueba con la utilización de técnicas de espionaje con la herramienta inSSIDer y captura de información desde el AP como nombre de la red o Service Set IDentifier (SSID), potencia de la señal (Strength), tipo de autenticación, cifrado y canal. Y para comprobar la robustez del cifrado de contraseñas en WEP, WPA y WPA2 se empleó la herramienta AirCrack. En Veizaga (2013), se aborda sobre cómo extraer claves con la herramienta.

DESARROLLO

El primer paso para asegurar una red WLAN es conocer cuáles son los tipos de ataques que puede afrontar. Estos pueden ser divididos en dos grandes grupos:

Los ataques pasivos: el objetivo del atacante es obtener información. Suponen un primer paso para ataques posteriores. Algunos ejemplos de este tipo son el espionaje, escuchas, wardriving y el descubrimiento de contraseñas.

Los ataques activos: implican modificar o crear falsos flujos de datos en la transmisión. Pueden tener dos objetivos diferentes, suplantar identidad o colapsar los servicios que presta la red. Algunos ejemplos son el spoofing, la instalación de AP no autorizados (Rogue APs), el ataque del hombre en el medio, el secuestro de sesiones (Hijacking) y la denegación de servicio (DOS) descritos en Pellejero, Andreu & Lesta (2004); y Flickenger (2008).

El segundo paso es el conocimiento de los protocolos de seguridad para redes WLAN, así como un análisis comparativo de aquellos con mayor aplicabilidad en este tipo de redes para limitar el número de vulnerabilidades. Se explican a continuación.

Protocolos de seguridad en redes WLAN

Los protocolos de seguridad que se pueden aplicar en redes WLAN son diversos, entre ellos están: privacidad equivalente al cableado (WEP), acceso protegido Wi-Fi (WPA), IEEE 802.11i y acceso protegido Wi-Fi2 (WPA2), aunque también se pueden utilizar otros mecanismos como las listas de control de acceso (ACL) que también se aplican a otros tipos de redes, pero al ser las redes inalámbricas, una extensión de las redes cableadas, puede ser aplicada a las mismas.

En cuanto a los protocolos de seguridad en redes WLAN existen dos aspectos fundamentales a tener en cuenta: la autenticación y el cifrado, por lo que este trabajo se centrará en ellos a la hora de establecer la comparación. El cifrado es el tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Suele emplearse para ello un algoritmo y una clave de cifrado (Pellejero, Andreu & Lesta, 2004).

La autenticación es el proceso de verificar y asegurar la identidad de las partes involucradas en una transacción. Mediante ella se evita que una entidad asuma una identidad falsa, comprometiendo la privacidad y la integridad de la información. En las redes WLAN es empleada para establecer la validez de una transmisión entre los APs y/o estaciones inalámbricas. IEEE 802.11 define dos tipos de servicio de autenticación: el sistema abierto y el de clave compartida.

En el método de autenticación abierta el dispositivo cliente envía un mensaje de solicitud de autenticación, al que el AP contesta con un mensaje de respuesta de autenticación. Al operar en este modo un AP acepta cualquier solicitud. Aunque, existe una variante donde en el AP puede realizarse un filtrado por direcciones MAC.

Filtrado por direcciones MAC

Como parte del estándar 802.11, cada dispositivo tiene una dirección MAC asignada por el fabricante. Para incrementar la seguridad inalámbrica es posible configurar en el AP una lista de direcciones MAC aceptando solo las MAC de los dispositivos autorizados a acceder a la red. Esta técnica tiende a ser compleja si es implementada en grandes organizaciones, puede consumir tiempo en configuración y mantenimiento, por lo que se recomienda su uso en redes pequeñas. Evita que los dispositivos que se encuentren dentro del área de cobertura del AP que no estén en el listado de direcciones MAC, puedan acceder a la red, lo cual permite prevenir accesos no autorizados (Chiu, 2006).

Por otra parte, proporciona un nivel bajo de protección, la suplantación de direcciones MAC vulneraría el sistema (Andra, 2010), permitiendo que se conecten dispositivos sin acceso a la red. Pues muchas tarjetas permiten cambiar su dirección MAC, ya sea mediante el valor que su controlador lee y almacena en memoria o reprogramando la propia tarjeta. Adicionalmente, existen utilidades que permiten obtener una MAC mediante la captura del tráfico de terminales conectados a la red. Además implica un esfuerzo adicional para la administración de la red ya que se deben mantener actualizadas las listas de direcciones MAC en cada AP.

WEP

WEP fue el primer protocolo de seguridad implementado bajo el estándar de redes inalámbricas IEEE 802.11 para cifrar los datos antes de ser enviados a través de la red. Los objetivos de WEP son proporcionar autentificación y confidencialidad en redes WLAN (Pellejero, Andreu & Lesta, 2004; Andra, 2010). En la actualidad la protección que ofrece es débil como se describe en Veizaga (2013). Esto es cuestionable ya que en el momento que fue diseñado no se pensó que despertaría el interés por los hackers que ha alcanzado. WEP provee autenticación abierta y de clave compartida (Cole, Krustz & Conley, 2005).

En la autenticación abierta en WEP, un cliente inalámbrico o un AP, provee un nombre incluido en los paquetes de una red WLAN para identificarlos como parte de la misma, este nombre se denomina SSID, y es común para los clientes inalámbricos y sus APs. Este SSID autoriza y asocia a un cliente inalámbrico al AP. Una vulnerabilidad de este mecanismo es que el AP transmite el SSID en texto plano durante intervalos en las tramas de gestión. De esta forma, el SSID está fácilmente disponible a los atacantes para establecer una asociación con el AP. En cuanto a la autenticación con clave compartida, el algoritmo de encriptación utilizado es RC4, donde los paquetes transmitidos son encriptados con una clave y un campo de chequeo de integridad (ICV) compuesto por una suma de comprobación CRC-32 adjuntada al mensaje como se describe en Barajas (2003); y Campbell, Calvert, Boswell & Hecht (2004).

El algoritmo provee una autenticación débil para la conexión de los clientes inalámbricos al AP, donde el AP no se identifica con los mismos. WEP autentifica clientes inalámbricos y no a usuarios de la red. Cuando se habilita, los clientes no pueden asociarse con el AP hasta que utilicen la clave correcta. El protocolo no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red (Campbell, Calvert, Boswell & Hecht, 2004).

Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida (Flickenger, 2008). Y por otro lado, la distribución manual de claves consume tiempo provocando que las claves no sean cambiadas periódicamente y que a menudo se deshabiliten las opciones de seguridad de los equipos para no tener que asumir el costo administrativo de poner las claves en los clientes inalámbricos.

La clave simétrica de WEP está conformada por dos componentes, un vector de inicialización (IV) y una clave compartida que puede ser de 40 o 104 bits. Debido a que la clave se cambia poco, el propósito del IV es frustrar el criptoanálisis en contra de WEP teniendo el cliente que usar un IV diferente para cifrar los paquetes del mensaje. Ambos extremos deben conocer tanto la clave como el IV. Sin embargo, al no ser grande el número de IVs diferentes, son $2^{24}2^{24}$=16.777.216 millones, terminarán repitiéndose en dependencia de la carga de la red. Permitiendo saber si dos tramas han sido cifradas con la misma clave, puesto que el IV se envía sin cifrar y la clave es estática. Por lo que monitoreando paquetes se mostrarán repeticiones del IV y permitirá a los atacantes obtener la clave como plantean Campbell, Calvert, Boswell & Hecht (2004).

En la Universidad de California (2015) se ha demostrado que la seguridad de WEP puede ser fácilmente quebrantada. Además, programas disponibles en internet como Aircrack pueden usarse para descifrar las claves y leer los mensajes transmitidos. Aircrack fue probado antes del desarrollo de este trabajo y comprobó los resultados antes mencionados. WEP es también vulnerable a ataques de falsificación y reenvío, en los cuales un atacante puede capturar o modificar paquetes y retransmitirlos posteriormente.

Otra de las debilidades en la implementación del IV en el protocolo es que el estándar 802.11 no especifica cómo manejarlo, plantea que el IV debería ser distinto en cada trama para mejorar la privacidad, pero no obliga a ello, queda en manos de los fabricantes cómo variar el IV en sus productos lo cual trae como resultado que en parte de las implementaciones, cada vez que arranca la tarjeta de red, el IV sea inicializado en 0 y se incrementa en 1 para cada trama, ocasionando que las primeras combinaciones de IVs y clave compartida se repitan frecuentemente. Esta probabilidad aumenta si se tiene en cuenta que cada cliente utiliza la misma clave compartida, por lo que las tramas con igual clave se multiplican en el medio.

Por otra parte, en las actualización de WEP a WEP2 se aumentó la clave a 128 bits, aunque en realidad lo que se aumentó es la clave que comparten los clientes con el AP de 40 a 104, pero el IV sigue siendo de 24 bits y padeciendo las debilidades del IV como se describe en Barajas (2003). Por lo cual el protocolo WEP2 permite deducir la clave al igual que WEP.

Una de las ventajas del uso del protocolo sobre el método de autenticación abierta con filtrado de direcciones MAC es que no es necesario mantener en los AP un listado actualizado con las direcciones MAC de los clientes inalámbricos. Otra es que debido al limitado poder de procesamiento con que se fabricaban los AP, que entre las

funciones de su hardware está cifrar cada paquete del mensaje, el algoritmo de encriptación RC4 no sobrecarga el hardware del AP por lo que no se convierte en una limitación implementarlo.

WPA

WPA es un protocolo de seguridad propuesto en el 2003 y desarrollado por la Wi-Fi Alliance para mejorar las debilidades encontradas en WEP, basado en el borrador del estándar IEEE 802.11i como describen Prasad & Prasad (2005); y Rumale & Chaudhari (2011). WAP hace uso del protocolo temporal de integridad de claves (TKIP) definido en el estándar 802.11i. TKIP usa RC4 para el cifrado y genera claves de 128 bits (seed) compartida entre dispositivos inalámbricos. Posteriormente esa clave se combina con la dirección MAC del usuario.

TKIP usa un IV de 48 bits, el cual es suficiente para transmitir 218.474.976.710.656 paquetes sin repetir el IV; asegurando que los usuarios utilicen claves diferentes en la encriptación de sus datos para mitigar los ataques del IV débil de WEP. TKIP implementa una función para mezclar claves que combina la clave compartida con el IV lo cual lo hace más robusto que WEP que concatena el IV con la clave compartida. TKIP incluye un mecanismo de chequeo de integridad del mensaje de 64 bits (MIC), conocido también como Michael, previniendo que intrusos capturen paquetes, los alteren y los reenvíen. MIC realiza un hash criptográfico a los valores del IV, calculado sobre las direcciones MAC origen, destino y texto plano (datos), el cual reemplaza el Checksum CRC-32 utilizado en WEP (García, 2011).

En WPA es posible emplear dos modos de autenticación diferentes en dependencia del entorno de aplicación:

WPA personal, con clave compartida para entornos residenciales y redes pequeñas: el usuario debe introducir una clave que puede tener de 8 a 63 caracteres configurada en el AP y en cada cliente, evita con ello ataques de escucha y accesos no autorizados. La clave se utiliza para iniciar la autenticación, no para el cifrado y permite una relación de acuerdo único para generar el cifrado TKIP en la red. Aunque la clave para la autenticación es común para todos los dispositivos de la red WLAN, no lo son las claves de cifrado, que son distintas para cada uno, constituye esto una mejora con respecto a WEP. En esta solución se recomienda que las claves estén constituidas por caracteres hexadecimales y que la longitud sea mayor que 20 caracteres para no ser descubiertas.

WPA empresarial, recomendado para entornos educativos, de negocios y gubernamentale: se basa en los mecanismos IEEE 802.1x y el protocolo de autentificación extensible (EAP). Donde, IEEE 802.1x es un estándar para el control de acceso basado en puertos que ofrece un marco para una autenticación basada en usuario y contraseña o certificados digitales y distribución de claves de cifrado. El mismo debe ser usado junto a cualquier tipo de EAP con generación de claves cifradas. Por su parte EAP definido en la RFC 2284, que quedó obsoleta por la RFC 3748 en junio del 2004 (Aboba, Blunk, Vollbrecht & Carlson, 2004) y actualizado por la RFC 5247 (Aboba, Simon & Eronen, 2008), es el protocolo que define las credenciales necesarias para la autenticación de usuarios, la autorización y la contabilidad creando un túnel seguro entre el AP y el servidor RADIUS.

Emplear EAP con IEEE 802.1x permite utilizar varios esquemas de autenticación entre clientes inalámbricos y la red en cuestión, entre los esquemas más comunes están: Radius, Kerberos, certificados digitales, autenticación mediante tarjetas inteligentes y tarjetas de identificación (SIM). Según el esquema será seleccionado el tipo de EAP con las credenciales necesarias para llevar a cabo la autenticación. EAP permite la generación, distribución y gestión de claves dinámicas. Entre los tipos de EAP existentes, los más seguros y flexibles son: EAP-TLS en el caso de seleccionar autenticación de cliente mediante certificados, PEAP y EAP-TTLS que permiten la autenticación del cliente mediante nombre de usuario y contraseña, PEAP es compatible con las soluciones de Microsoft (Remote Authentication Dial In User Service (Radius) y Active Directory), y EAP-TTLS que se puede utilizar con mayor número de mecanismos de autenticación como FreeRadius y LDAP.

El conjunto de estos dos mecanismos unido al esquema de cifrado forman una fuerte estructura de autenticación que utiliza un servidor de autenticación centralizado, generalmente un servidor RADIUS que es un protocolo de red que provee administración centralizada con autenticación, autorización y contabilidad. Los proceso de autenticación y autorización son definidos en la RFC 2865 (Rigney, Willens, Rubens & Simpson, 2000) y actualizados en la RFC 5080 (Nelson & DeKok, 2007) y la RFC 6929 (DeKok & Lior, 2013) mientras que el proceso de contabilidad es descrito en la RFC 2866 y actualizado en la RFC 5080 (Nelson & DeKok, 2007) y la RFC 5997 (DeKok, 2010). RADIUS permite usar una base de datos de usuarios, para almacenar sus nombres y contraseñas. Algunas de estas bases de datos son Microsoft Active Directory, MySQL, PostgreSQL y LDAP.

Una de las ventajas de usar WPA es que emplea el mismo algoritmo de cifrado RC4 que WEP, por lo que en una red WLAN con equipamiento WEP, solo es necesario una actualización del software en los clientes inalámbricos y en

los AP, sin llevar a cabo cambios de hardware. También implementa un contador de secuencia para protegerse contra los ataques de reenvío frecuentes en WEP. TKIP implementa un mecanismo de intercambio de claves que asegura que todos los paquetes sean enviados con una única clave de encriptación.

En cuanto al algoritmo de cifrado, tanto WEP como WPA emplean el algoritmo RC4, se ha demostrado que es vulnerable a ataques. Aunque en el caso de WPA disminuye las vulnerabilidades conocidas de WEP, ya que TKIP utiliza RC4 con claves de 128 bits para el cifrado la cual fue aumentada respecto a WEP que es de 64 y se mantuvo de igual tamaño respecto a WEP2, pero con un aumento del IV de 24 bits en WEP a 48 en WPA, además el empleo de TKIP incorpora el hash de claves por paquete MIC y la rotación de claves de difusión, lo que protege la red WLAN de ataques de clave débil que ocurrían en WEP.

IEEE 802.11i

EL estándar IEEE 802.11i define mejoras de seguridad mediante el estándar de cifrado avanzado (AES) y procedimientos de autentificación para complementar y mejorar la seguridad en redes WLAN proporcionada por WEP. El estándar abarca 3 nuevos algoritmos de encriptación: TKIP basado en RC4 compatible con el hardware actual, AES, el cual es un algoritmo robusto pero requiere de un mayor poder de cálculo que RC4, y 802.1x/EAP para la autenticación como plantean Prasad & Prasad (2005); y Pantoja (2004). En el caso de IEEE 802.11i la técnica empleada para superar la vulnerabilidad del IV de WEP es el protocolo Counter Mode with CBC-MAC Protocol (CCMP), en el que se utilizan IV de 48 bits al igual que en TKIP.

WPA2

Implementación aprobada por Wi-Fi Alliance de IEEE 802.11i. El grupo WPA2 de la Wi-Fi Alliance es el grupo de certificación del estándar IEEE 802.11i. El Instituto de Ingenieros Eléctrico y Electrónicos IEEE propone WPA2 como la solución definitiva al problema de seguridad en redes WLAN ante las debilidades encontradas en WEP. La versión oficial del estándar fue ratificada en junio del 2004. WPA2 es más seguro que WPA porque usa como mecanismo de encriptación AES que soporta claves de 128 bits, 192 bits y 256 bits en lugar de RC4/TKIP, y porque reemplaza el algoritmo Michael por el protocolo CCMP, que es considerado criptográficamente seguro. WPA2 puede ser usado al igual que WPA con autenticación de clave compartida o en entornos empresariales (IEEE 802.11i/EAP) que permite autenticación RADIUS (Rumale & Chaudhari, 2011).

Las redes WLAN basadas en WPA2 son consideradas las más seguras. Aunque, en modo personal la difusión y multidifusión de claves representan una vulnerabilidad. Todos los nodos de la red necesitan conocerlas, y un atacante puede descubrir la clave mediante el intercambio entre el AP y el cliente. Se recomienda emplear WPA2 Empresarial en caso de que se necesite confidencialidad mediante el cifrado a nivel de enlace. En caso de usarse una solución más simple como WPA2 personal, deben tomarse precauciones al escoger la clave. En WPA2 como el cifrado se basa en el algoritmo AES no sufre de los problemas asociados con RC4. Pero por otra parte requiere poder de procesamiento por lo que se hace necesario actualizar el hardware existen en la red WLAN en caso de que no lo soporte.

Otros protocolos de seguridad aplicables a redes WLAN

Adicionalmente, a los mecanismos vistos anteriormente es posible emplear en redes WLAN otros protocolos usados en otros tipos de redes como: SSH, HTTPS y SSL. Es importante aclarar que existen más pero este trabajo considera estos como los más empleados.

Protocolos SSL, SSH y HTTPS

En redes WLAN pueden ser aplicados otros protocolos como SSL, SSH y HTTPS. El protocolo SSL, cuya versión actual es la 3.0 presentada en 1996 por la IETF en la RFC 6101 (Freier, Karlton & Kocher, 2011), es un protocolo criptográfico diseñado para proveer comunicaciones seguras en internet. El cual se basa en el uso de certificados digitales y se ha convertido en el estándar de facto para transacciones Web seguras. HTTPS es la versión segura de HTTP que utiliza un cifrado basado en SSL para crear un canal más apropiado para el tráfico de información sensible que el protocolo HTTP. SSL y HTTPS permiten asegurar la comunicación mediante el acceso web entre cliente y servidor, protegiendo el proceso de autentificación con certificados que posibilita que con herramientas como el firebug que es un plugin para Firefox, con el cual se pueden observar los datos transferidos entre clientes y servidores web, no puedan obtenerse el usuario y la contraseña durante la conexión. En el caso del protocolo Secure Shell (SSH), sirve para acceder a máquinas remotas usando técnicas de cifrado a través de un canal SSH para que un atacante no pueda descubrir el usuario y la contraseña, ni lo que se escribe durante la conexión a los servidores.

Propuesta de protocolos de seguridad para la red WLAN de la UCF

Después de identificados los principales protocolos de seguridad en redes WLAN y realizada una comparación

de los mismos. Se propone para la red WLAN de la UCF una solución de seguridad basada en WPA2 empresarial, empleando 802.1x y EAP-PEAP para autenticar a los usuarios con sus credenciales mediante un servidor Radius, el cual usará la base de datos del Active Directory por razones de tiempo, pues en ella se encuentran registrados los usuarios de la UCF; permite servicios de autenticación, autorización y contabilidad que son de interés para la administración de la red en la universidad.

En el caso de la UCF se decide emplear WPA2 empresarial porque al establecer la comparación resultó ser el más seguro de los protocolos y el modo empresarial, el más seguro de implementarlo. Además el equipamiento fue comprado recientemente, son APs del fabricante NETGEAR modelo WNAP320 compatible con los estándares 802.11 b/g/n y que implementan soporte para WPA y WPA2 en modo empresarial, emplea Radius basado en autenticación 802.1x y autentificación mediante certificados, así como generación dinámica de claves de encriptación.

En caso contrario que los AP no soporten WPA2 y soporten WEP y/o WPA la solución pudiera ser actualizar todo el equipamiento que se pueda a WPA y emplear este para el control de acceso al medio. Como se ha visto anteriormente una de las principales diferencias entre WPA2 y WPA se encuentra en el algoritmo de cifrado utilizado, IEEE 802.11i/WPA2 utilizan AES, y WPA al igual que WEP, utiliza RC4. Por lo que pueden existir AP que soporten el modo mixto WEP-WPA, pero no que soporten el modo mixto WEP-IEEE 802.11i/WPA2.

En esta solución la red WLAN de la UCF está compuesta por la subred WLAN en cuestión y la red de distribución de servicios inalámbricos, esta última es una red cableada que interconecta los dispositivos que brindan servicios a la red inalámbrica. Se recomienda dedicar una red de área local virtual (VLAN) para la red de distribución de servicios inalámbricos dentro de la red LAN corporativa y no compartirla con una subred LAN para poder realizar filtrados entre VLANs y proteger los servidores del núcleo de la red de ataques DoS.

Los servicios que se desea prestar a los usuarios inalámbricos deben ubicarse en una DMZ que retransmita las peticiones a los servidores de la empresa. Se propone implementar un firewall entre la subred inalámbrica, que debe considerarse insegura y la red corporativa para filtrar el tráfico, un servidor DHCP para proporcionar las configuraciones IP a los clientes inalámbricos aumentando la escalabilidad de la red y un servidor DNS. Para la administración remota a los servidores, emplear SSH con el objetivo de proteger las credenciales de administración. Además, en el caso de servidores como SIGENU, Moodle y Active Directory, tanto como para los APs será implementada una ACL centralizada para registrar las direcciones MAC y los puertos de acceso de las PC donde radica el personal con permiso administrativo en el servidor con el objetivo de limitar el acceso desde PC no autorizadas. Y para acceder a servidores web donde se gestionen las credenciales de usuario se usará SSL, como, por ejemplo, el acceso al servidor de correo mediante un cliente web. La Figura 1 muestra cómo quedaría la arquitectura de la red WLAN de la UCF empleando WPA2 en modo Empresarial.

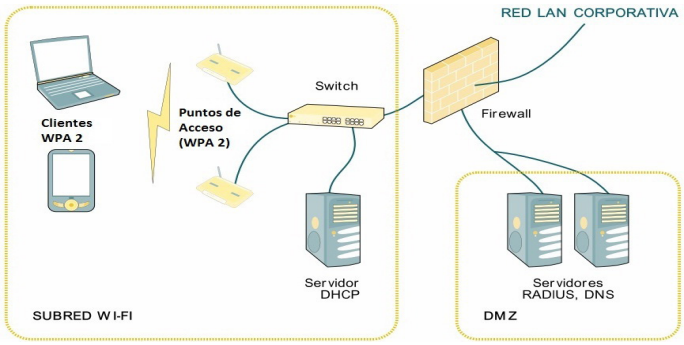

Figura 1. Propuesta de arquitectura para la UCF, modificado de Pellejero, Andreu & Lesta (2004).

CONCLUSIONES

Las redes inalámbricas se han convertido en una alternativa a las redes LAN cableadas para facilitar la movilidad y llegar a lugares donde el cableado no es posible. Pero se hace necesario tener en cuenta los protocolos de seguridad debido a que las transmisiones viajan por un medio no seguro (el aire).

Existen diversos mecanismos de seguridad para redes LAN como SSH, HTTPS, SSL que pueden ser aplicados a redes WLAN. En redes WLAN se puede llevar a cabo la autenticación de terminales de usuario basándose en su dirección MAC, pero en este mecanismo de seguridad la información no es enviada de forma cifrada, la escalabilidad se hace compleja al incrementar el número de dispositivos clientes y es vulnerable.

El sistema WEP posee debilidades, por lo que deben buscarse alternativas. Una puede ser actualizar el equipamiento a WPA, ya que aunque el algoritmo de cifrado WPA ha sido vulnerado solo es posible realizar ataques que comprometan la información cifrada en WPA personal. El modo WPA empresarial no ha sido vulnerado.

El estándar WAP2 demostró ser la alternativa más segura para campus universitarios como el de la UCF donde

se requiere autentificar y auditar a sus usuarios con sus credenciales. No hay una solución estándar de seguridad para redes WLAN. Es necesario identificar los requisitos de seguridad que se quieren alcanzar y sobre la base de los mismos emplear los protocolos combinándolos, según las necesidades.

REFERENCIAS BIBLIOGRÁFICAS

Aboba, B., Blunk, L., Vollbrecht, J., & Carlson, J. (2004). Extensible Authentication Protocol (EAP). ***RFC 3748***. Recuperado de https://tools.ietf.org/html/rfc3748

Aboba, B., Simon, D., & Eronen, P. (2008). Extensible Authentication Protocol (EAP) Key Management Framework. ***RFC 5247***. Recuperado de https://tools.ietf.org/html/rfc5247

Barajas, S. (2003). Protocolos de seguridad en redes inalámbricas. Recuperado de http://www.saulo.net/pub/inv/SegWiFi-art.htm

Campbell, P., Calvert, B., Boswell, S., & Hecht, H. (2004). ***Security+ Guide to Network Security Fundamentals***. London: Atlantic Books.

Chiu, S. H. (2006). Seguridad en Redes Inalámbricas 802.11. Recuperado de http://www.ciens.ucv.ve:8080/genasig/sites/redesmov/archivos/Seguridad%20en%20Redes%20Inalambricas%20802.pdf

Cole, E., Krustz, R., & Conley, J. W. (2005). ***Network Security Bible***. Indianapolis: Wiley Publishing, Inc.

DeKok, A. (2010). Use of Status-Server Packets in the Remote Authentication Dial In User Service (RADIUS) Protocol. ***RFC 5997***. Recuperado de https://tools.ietf.org/html/rfc5997

DeKok, A. L., & Lior, A. (2013). Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions. ***RFC 6929***. Recuperado de https://tools.ietf.org/html/rfc6929

Filip, A., & Vázquez Torres, E. (2010). Seguridad en redes WiFi Eduroam. Recuperado de http://trajano.us.es/docencia/RedesYServiciosDeRadio/2010/Seguridad%20en%20redes%20Wifi%20Eduroam.pdf

Flickenger, R. (2008). ***Redes Inalámbricas en los Países en Desarrollo***. Seattle: Hacker Friendly LLC.

Freier, A., Karlton, P., & P. Kocher. (2011). The Secure Sockets Layer (SSL) Protocol Version 3.0. ***RFC 6101***. Recuperado de https://tools.ietf.org/html/rfc6101

García, R. R. (2011). ***Arquitectura para el Control de Acceso de la Red inalámbrica local de la Universidad Central "Marta Abreu" de Las Villas.*** Santa Clara: Universidad Central "Marta Abreu" de Las Villas.

Institute of Electrical and Electronics Engineers. (2004). IEEE Standards Association. Recuperado de http://standards.ieee.org/findstds/standard/802.11i-2004.html

Nelson, D., & DeKok, A. (2007). Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes. ***RFC 5080***. Recuperado de https://tools.ietf.org/html/rfc5080

Pellejero, I., Andreu, F., & Lesta, A. (2004). ***Seguridad en redes WLAN***.

Prasad, N. R., & Prasad, N. R. (2005). ***802.11 WLANs and IP Networking. Security, QoS, and Mobility***.Londo: Artech House. Recuperado de http://dlia.ir/Scientific/e_book/Technology/Electrical_Nuclear_Engine_Electronics/TK_5101_6720_Telecommunication_/021341.pdf

Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2000). Remote Authentication Dial In User Service (RADIUS). ***RFC 2865***. Recuperado de https://tools.ietf.org/html/rfc2865

Rigney, C. (2000). RADIUS Accounting. ***RFC 2866***. Recuperado de https://tools.ietf.org/html/rfc2866

Rumale, A.S., & Chaudhari, D. N. (2011). IEEE 802.11x, and WEP, EAP,WPA / WPA2. Tech. Appl, 2 (6), pp. 1945-1950. Recuperado de http://www.ijcta.com/documents/volumes/vol2issue6/ijcta2011020634.pdf

United State of América. University of California.(2015). WEP FAQ. Recuperado de www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Veizaga, W. J. B. (2013). Ethical Hacking: Hacking de Red Inalámbrica Wifi. ***Carrera de Informática***, pp. 2-3.