Análisis de la criptografía aplicada en las comunicaciones Wi-Fi

Juan Carlos Sendón Varela[1]
Jorge Herrera-Tapia[2]
Lytyet Fernández Capestany[3]
Jorge Pincay Ponce[4]

Resumen

En este trabajo tiene como objetivo revisar bibliográficamente elementos relevantes asociados con la criptografía de los protocolos de seguridad más conocidos a nivel de redes inalámbricas con los estándares Wireless Fidelity (Wi-Fi), los mismos que buscan garantizar la confidencialidad e integridad de la información que se transmite en las redes de comunicaciones. Se realiza un análisis de trabajos relacionados en aspectos cruciales como son la formulación conceptual de los protocolos de comunicación inalámbricos, aspectos relacionados a la seguridad en redes inalámbricas con los fundamentos a tener en cuenta sobre la criptografía, así como los protocolos de seguridad que se implementan en redes Wi-Fi. También son tratados los riesgos y vulnerabilidades asociados a las características específicas de los protocolos de seguridad de las redes móviles. Esta información se presenta de una manera clara y sencilla para que sea comprendida sin la dificultad que este tipo de investigaciones tecnológicas supone. Los resultados alcanzados evidencian la atención que la comunidad científica está dando a esta temática y la necesidad de continuar profundizando en su estudio, lo que justifica su importancia y actualidad para acceder y compartir recursos manera segura en Internet.

Palabras clave: Criptografía, seguridad redes inalámbricas.

[1] Profesor Universidad Laica Eloy Alfaro de Manabí – Ecuador. E-mail juan.sendon@live.uleam.edu.ec
[2] Profesor Universidad Laica Eloy Alfaro de Manabí – Ecuador. E-mail jorge.herrera@live.uleam.edu.ec
[3] Profesor Universidad Laica Eloy Alfaro de Manabí – Ecuador. E-mail lytyet.fernandez@uleam.edu.ec
[4] Profesor Universidad Laica Eloy Alfaro de Manabí – Ecuador. E-mail jorge.pincay@live.uleam.edu.ec

Introducción

En la actualidad, las redes inalámbricas de área local (Wireless Local Area Network WLAN) son parte fundamental en las comunicaciones entre equipos informáticos. Por su facilidad de instalación, administración y conexión se han convertido en una excelente solución para ofrecer conectividad en aquellos lugares donde resulta difícil brindar servicios de telecomunicaciones con una red cableada. Además, la popularidad y aceptación de estos tipos de conexión ha crecido de tal manera que muchos fabricantes de hardware hoy en día incorporan acceso inalámbrico en sus equipos (Madrid Molina, 2006).

Fidelidad inalámbrica, Wireless Fidelity (Wi-Fi), referencia para WiFi en inglés, se incluye dentro de la IEEE 802.11a/b/g/c, normas para WLAN y permite a los usuarios navegar por Internet a velocidades de banda ancha cuando está conectado a un punto de acceso (AP) o en modo ad-hoc.

Sin embargo, desde el punto de vista de la seguridad, los puntos de acceso inalámbricos presentan una serie de dificultades. Una vez que un atacante ha comprometido un punto de acceso, se puede tanto espiar así como inyectar tráfico a los usuarios en la red inalámbrica. Para solucionar estos problemas, los protocolos de seguridad como WEP, WPA y WPA2 (IEEE 802.11i) han sido replanteados en los últimos años, sin embargo, se tienen muchas evidencias de que han sido comprometidos y presentan vulnerabilidades (Xiong & Jamieson, 2010).

El presente trabajo tiene como objetivo analizar los principales algoritmos de la seguridad en redes de datos inalámbricas del tipo Wi-Fi desde una perspectiva conceptual, citando las principales vulnerabilidades criptográficas en protocolos de seguridad que podrían poner en riesgo la seguridad informática de una organización.

Redes inalámbricas

Las redes inalámbricas del tipo Wi-Fi fueron desarrolladas en primera instancia para proporcionar conectividad dentro de redes locales, en la actualidad se ha convertido en la principal tecnología en la capa de acceso a Internet, por su fácil despliegue al nivel de costos e instalación. Entre las principales desventajas de este tipo de redes están el mayor consumo de energía, amenazas a la seguridad

de datos debido a las propiedades inherentes del medio de transmisión, las preocupaciones sobre la seguridad del usuario debido a la continua exposición a la radiofrecuencia, y bajas velocidades de datos (Ferro & Potortì, 2005).

Seguridad en redes inalámbricas

La privacidad en la transferencia de datos a través de redes inalámbricas es compleja, teniendo en cuenta que la comunicación inalámbrica es siempre susceptible de ser interceptada por cualquiera dentro del espectro de la señal inalámbrica, que por su naturaleza son vulnerables a muchas amenazas, como accesos no autorizados, escucha de la comunicación, modificación, denegación de servicio, la repetición de los datos e inyección de los mismos (Arora & Khera, 2015; Bhatia & Sumbaly, 2014).

Si bien en una red Wi-Fi, se puede utilizar una gran variedad de métodos y procedimientos que protejan la red inalámbrica, como el cambio del nombre de fábrica de la red, eliminación de la difusión del identificador de la red (SSID), entre otros; también se pueden emplear tecnologías más sofisticadas y técnicas de encriptación como WEP, WPA y WPA2. A continuación se explicarán algunos conceptos relacionados a la seguridad de las redes.

Criptografía

Según (Schneier, 2013) la realidad de la seguridad es matemática, en base a la probabilidad de diferentes riesgos y la eficacia de las diferentes medidas. Por otra parte (Bhatia & Sumbaly, 2014) plantean que la seguridad en redes inalámbricas, depende del secreto de todo el proceso de cifrado y descifrado. Y la criptografía, se encarga del estudio de las técnicas y las prácticas de las comunicaciones seguras, cuando existe la amenaza de adversarios o terceros, que pueden poner en peligro la integridad de la información y está sustentada por la criptografía y el criptoanálisis.

El criptoanálisis, se refiere al estudio de los criptosistemas con el fin de encontrar debilidades en los que van a permitir la recuperación del mensaje original del cifrado mensaje, sin el conocimiento de la clave o el algoritmo utilizado (Bhatia & Sumbaly, 2014). Los algoritmos de criptografía se dividen en dos tipos dependiendo de la distribución de las claves, algoritmos de clave simétrica y algoritmos de clave asimétrica o también conocido como de clave pública.

Criptografía de clave simétrica

Los criptosistemas que usan la misma clave para el cifrado y descifrado se denominan de clave simétrica o de clave secreta y la distribución de las claves simétricas son pre distribuidas a cada par de sistema de comunicación, ver Figura 1 (Bhatia & Sumbaly, 2014).

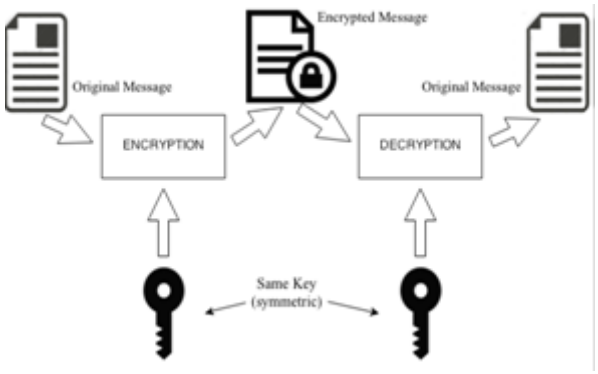

Figura 1. Criptografía de clave simétrica.

Fuente: (Bhatia & Sumbaly, 2014).

Criptografía de clave asimétrica

Por otro lado, los criptosistemas que hacen uso de la distribución de claves asimétricas utilizan un sistema de clave pública que consta de dos partes: una clave privada, que se mantiene secreta y una clave pública, que se distribuye a través de la red. El que envía el mensaje cifra el mismo utilizando la clave pública del receptor. Por otro lado, el receptor hace uso de su clave privada para descifrar el mensaje. La clave privada nunca de transmite por el canal de comunicación, por tanto, es menos vulnerables a los problemas de seguridad. La Figura 2. muestra el proceso de la criptografía de clave asimétrica (Balitanas, 2009; Bhatia & Sumbaly, 2014).

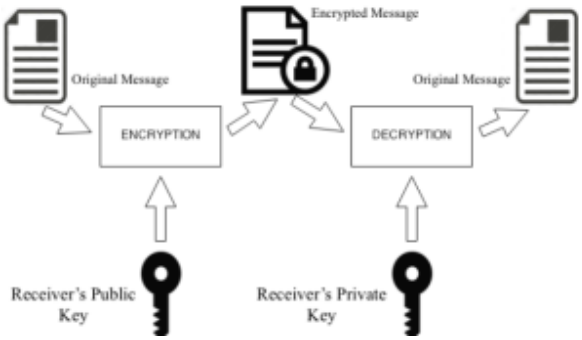

Figura 2. Criptografía de clave asimétrica.

Fuente: (Bhatia & Sumbaly, 2014).

Protocolos de seguridad inalámbrica para redes Wi-Fi

Una vez que un cliente está conectado a un AP que ha sido comprometido por un atacante, su tráfico puede ser interceptado, y se podría introducir tráfico en la red cableada. Para contrarrestar esto, se ha propuesto protocolos de seguridad como como WEP, WPA y WPA2.

Algoritmo WEP

El protocolo de seguridad WEP (Wired Equivalent Privacy), fue el primer protocolo de cifrado introducido en el estándar IEEE 802.11 en el año 1999. (IEEE, 2012; Lehembre, 2006). WEP es un algoritmo opcional de seguridad incluido en la norma para Wi-Fi para proporcionar confidencialidad, autentificación y control de acceso entre el cliente y el punto de acceso (AP), en una red (Barajas, 2004).

Además, WEP utiliza criptografía simétrica entre las estaciones y el punto de acceso (AP), sin un mecanismo automático de distribución de la clave, por lo tanto, es necesario escribir la clave manualmente en cada uno de los dispositivos de la red inalámbrica originando problemas de seguridad ya que la clave estaría almacenada en todos los equipos de la red con la posibilidad de que sea conocida por un elemento externo, además este mecanismo de distribución de la clave provocaría un aumento de administración en la red, ocasionando que la clave cambie poco o casi nunca (Barajas, 2004; Boncella, 2002).

Del mismo modo, (Ahmad, Rajan, & Govardhan, 2012) concluyen que el protocolo WEP suministra tanto la autenticación como los servicios de cifrados. En el primer caso, la autenticación, como se describe en la Figura 3, va a proteger a la red contra los accesos no autorizados bajo un método de sistema abierto o con la autenticación de la clave compartida. Por otro lado, el cifrado que utiliza WEP en su implementación está basado en un cifrado de flujo de clave simétrica llamado RC4 con claves de 40 bits o 104 bits.

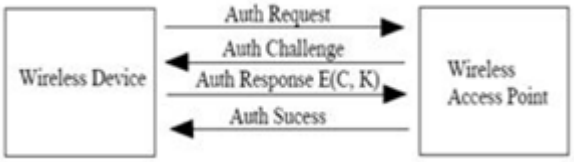

Figura 3. Autenticación WEP.

Fuente: (Ahmad et al., 2012).

Según (Barajas, 2004; Boncella, 2002) el algoritmo de cifrado RC4, utiliza claves de 64 bits, que están conformados por 24 bits pertenecientes al vector de inicialización (IV). El IV, se genera automáticamente y debería ser diferente para cada trama que se transmite, con el objetivo de cifrar con claves diferentes para que un posible atacante no pueda deducir la clave secreta del tráfico en la red, ver Figura 4. Así como no es complejo el proceso de cifrado de WEP, el descifrado tampoco lo ha sido, convirtiéndose en un protocolo vulnerable.

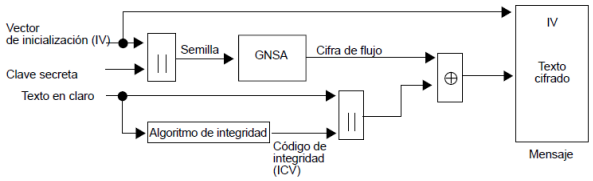

Figura 4. Cifrado WEP.

Fuente: (Madrid Molina, 2006).

Algoritmo WPA

El estándar WPA (Wi-Fi Protected Access), aparece en 2003, para resolver los problemas de seguridad presentado por el protocolo WEP y, por otro lado, no renunciar del todo a las tarjetas inalámbricas y puntos de accesos que utilizan WEP para su cifrado y que están siendo utilizadas (Barajas, 2004).

La razón principal por la WPA se impone sobre WEP es que el primero, permite una cifrado más complejo de los datos en el protocolo TKIP (Temporal Key Integrity Protocol) con la asistencia del código MIC que es la de evitar los ataques de tipo de bit-flipping fácilmente aplicados con WEP (Lashkari et al., 2009).

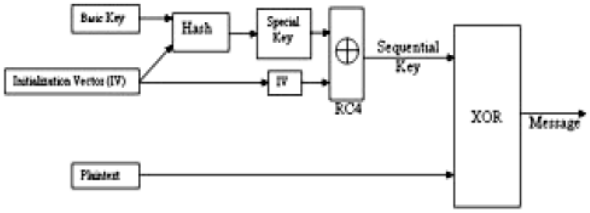

Figura 5. Algoritmo de cifrado WPA (TKIP).

Fuente: (Lashkari et al., 2009).

La Figura 5, describe el algoritmo TKIP. Este utiliza la técnica de cifrado RC4 como WEP, a diferencia que antes de que el vector de inicialización entre en el proceso del algoritmo RC4, este se duplica, uno pasa por un hash junto a la clave y el otro es enviado directamente a RC4. Luego de realizar el hash, el resultado es la clave que va a unirse a la otra copia del vector de inicialización, se produce la operación del algoritmo RC4 dando como resultado la clave secuencial que será operada con un XOR junto al texto plano y ahí estaría listo para enviar al receptor (Lashkari et al., 2009).

Algoritmo WPA2

El estándar 802.11i, también conocido por WPA2 de la WIFI Alliance surge para resolver los problemas que presenta WPA, cambiando el esquema de cifrado a AES-CCMP. Este algoritmo de cifrado llamado AES (Advanced Encryption Standard) es muy robusto, por esa razón fue adoptado como estándar de privacidad por el National Institute of Standards and Technology (NIST), para instituciones de gobierno de EEUU (R Castro, 2005).

Para garantizar la integridad y autenticidad de los mensajes WPA2 utiliza CCMP (Counter Mode with CBC-MAC Protocol) siendo un esquema de cifrado que utiliza AES que es un algoritmo de clave simétrica para cifrado de bloque muy seguro y robusto utilizando claves de 128 bits, vector de inicialización de 48 bits y no es compatible con esquemas anteriores como sucedía con TKIP (Barajas, 2004; R Castro, 2005).

Los autores de (Lehembre, 2006), exponen la nueva arquitectura para las redes inalámbricas, la Robust Security Network (RSN) utilizando autenticación 802.1X basada en EAP, distribución de claves robustas y nuevos mecanismos de integridad y privacidad.

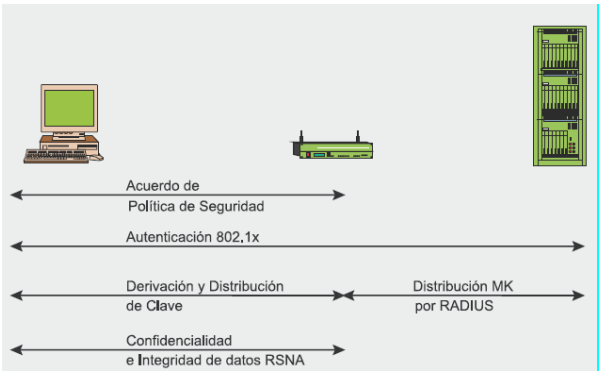

Figura 6. Fases de operación de 802.11i.

Fuente: (Lehembre, 2006)

También, podemos ver que WPA2 consta de cuatro fases, Figura 6; a lo que se le llama handshake o saludo de 4 vías para el establecimiento de la comunicación: i) acuerdo sobre la política de seguridad, ii) autenticación 802.1X, iii) derivación y distribución de las claves y, por último, iv) confidencialidad e integridad de los datos RSNA (Lehembre, 2006).

Vulnerabilidad de los Protocolos de seguridad en redes inalámbricas Wi-Fi. WEP, WPA y WPA2

A continuación, realizaremos un análisis con respecto a las vulnerabilidades que se presentan en estos tres estándares de seguridad en la comunicación inalámbrica.

Vulnerabilidades en WEP

En el caso de WEP, existen defectos que el atacante podría utilizar para violentar la red, uno de estos es el envío de IV (Vector de inicialización) en texto plano con el mensaje cifrado, de ahí que, un intruso que obtiene el tráfico de la comunicación, con herramientas como *Aircrack*, podría obtener información de los tres primeros caracteres o la clave secreta, incluso descifrar el dato sin conocer la clave secreta, teniendo en cuenta que la operación XOR es un proceso simple y se puede deducir un valor oculto si se conocen los otros dos (Kumkar et al., 2012).

El mecanismo de protección para las redes inalámbricas WEP, no incluye autenticación de usuario, más bien garantiza una autenticación de estación, entrando aquellos dispositivos que tengan guardada la configuración y la clave privada. Además, el enviar la clave cifrada con el IV y también, enviar el IV en texto

claro, evidencia una debilidad en el mecanismo, permitiendo que un hacker pueda recuperar la clave.

Vulnerabilidades en WPA

Desafortunadamente el protocolo de seguridad inalámbrico WPA no está libre de problemas. El más destacado es el ataque de negación de servicio (DoS). Este se origina durante proceso de 4-Way Handshake o saludo de 4 vías, esto se debe a que, en este proceso se envía el primer mensaje sin autenticar y un atacante podría aprovecharse de esta vulnerabilidad y suplantar la identidad de la víctima, conocido normalmente como *spoofing*, y se podría realizar un ataque *DoS* sobre el cliente si es posible que existan varias sesiones simultáneas. De esta vulnerabilidad, se dieron cuenta Changhua He y John C. Mitchell. Como consecuencia de lo anterior, si un atacante de la red envía paquetes seguidos en el mismo intervalo de tiempo errando en la clave, el AP elimina todas las conexiones de los clientes por el plazo de un minuto. Este mecanismo de defensa puede originar muchos inconvenientes y afecta la disponibilidad de la información (Lehembre, 2006).

Existen herramientas en ambiente Linux, que explotan vulnerabilidades en WPA y ejecuta ataque de autenticación. Estas herramientas llevan a cabo un ataque por fuerza bruta de diccionario, a diferencia de WEP, donde los métodos estadísticos pueden utilizarse para agilizar el proceso de ataque, contra WPA-PSK con el objetivo de obtener la frase de la contraseña compartida.

Vulnerabilidades en WPA2

Si bien el protocolo WPA2 para la proteccion de redes inalámbricas es bastante seguro, se pueden detectar determinadas vulnerabilidades que ponen en riesgo la seguridad de la información. (Rajotiya & Arora, 2012) nos menciona que si bien *WPA2* usa *AES* como algoritmo de encriptacion, mantiene el uso de TKIP, para conservar la compatibilidad con el hardware de WPA.

A consecuencia de lo anterior, WPA2 presenta el mismo problema que WPA con repecto al ataque de autenticación. (Rajotiya & Arora, 2012) señalan algunas de la vulnerabilidades que se presenta con este protocolo, como la imposibilidad de prevenir ataque en la capa fisica como la de inundacion. El método utilizado para

llevar a cabo este ataque es el de *Hombre en el Medio* (MitM), en el que el atacante se coloca entre las dos partes que realizan la comunicación.

Finalmente, si bien en WPA2 se presentan vulnerabilidades que afectan a otros mecanismos estándar de 802.11i, como son los ataques con suplantación de mensajes 802.1X, debido a una falla de autenticación, es importante destacar que el uso del protocolo no tiene protección alguna frente a ataques de intercepción de frecuencias de radio y negación del servicio a través de violaciones de 802.11, no analizadas en este documento (Lehembre, 2006).

Debido a lo vulnerable de WPA2, Wi-Fi Alliance ha diseñado una nueva generación de protocolos seguros para redes inalámbricas, la WPA3, que abordan varias deficiencias del estándar anterior, por ejemplo, la vulnerabilidad KRACK recientemente descubierta.

Conclusiones

Partiendo de los elementos señalados en este documento es posible extraer algunas conclusiones importantes acerca del alcance y vulnerabilidades de los protocolos WEP, WPA y WPA2 en su papel de protocolos que garantizan la seguridad de la información en las redes inalámbricas Wi-Fi.

En lo que respecta a WEP, este no aporta seguridad contra diversas amenazas, por esto, WPA fue una solución a los problemas de seguridad conocidos en WEP. Finalmente, WPA2 se aparece para superar los defectos de la WPA, este brinda un cifrado más seguro mediante el uso de bloques de cifrado AES, pero todavía es vulnerable a ataques debido al mecanismo de distribución de la clave GTK y la transmisión de las tramas de administración y control sin cifrar.

Se espera que con el nuevo protocolo WPA3 se cubran las vulnerabilidades de sus antecesores, y combinado con las mejores prácticas de seguridad se garantice un acceso seguro y la privacidad de los datos de los usuarios de Internet.

BIBLIOGRAFÍA

Ahmad, S. M. K. M. A., Rajan, E. G., & Govardhan, A. (2012). Attack Robustness and Security Enhancement with Improved Wired Equivalent Protocol, *03*(02). http://doi.org/01.IJNS.03.02

Arora, A., & Khera, A. (2015). Wi-Fi Enabled Personal Computer Network Monitoring System Using Smart Phone with Enhanced Security Measures. *Procedia Computer Science*, *70*(May), 114–122. http://doi.org/10.1016/j.procs.2015.10.052

Barajas, S. (2004). Protocolos de seguridad en redes inalámbricas. *Universidad Carlos III de Madrid*, 1–5. Retrieved from http://www.saulo.net/des/SegWiFi-art.pdf

Bhatia, P., & Sumbaly, R. (2014). Framework for Wireless Network Security Using Quantum Cryptography. *International Journal of Computer Networks & Communications*, *6*(6), 45–61. http://doi.org/10.5121/ijcnc.2014.6604

Boncella, R. J. (2002). Wireless security: an overview. *Communications of the Association for Information*, *9*, 269–282. Retrieved from http://washburn.edu/faculty/boncella/WIRELESS-SECURITY.pdf

Castro, R. (2005). Avanzando en la seguridad de las redes WIFI Going forward more Secure WIFI Networks. *Boletín de La Red Nacional de I+D RedIRIS*, (Nº. 73), 23–32. Retrieved from http://www.rediris.es/rediris/boletin/73/enfoque1.pdf

Ferro, E., & Potortì, F. (2005). Bluetooth and Wi-Fi wireless protocols: A survey and a comparison. *IEEE Wireless Communications*.

Kumkar, V., Gupta, A., Shrawne, S., Tiwari, A., & Tiwari, P. (2012). Vulnerabilities of Wireless Security Protocols (WEP and WPA2). *International Journal of Advanced Research in Computer Engineering & Technology*, *1*(2), 34–38.

Lashkari, A. H., Mohammad, M. I. R., Danesh, S., & Samadi, B. (2009). A Survey on Wireless Security protocols (WEP , WPA and WPA2 / 802 . 11i). *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, (IV), 48–52. http://doi.org/10.1109/ICCSIT.2009.5234856

Lehembre, G. (2006). Seguridad WI-FI WEP, WPA y WPA2. *Hakin9*, (1), 12–26. Retrieved from www.zero13wireless.net/wireless/ seguridad/01_2006_wpa_ES.pdf \nhttps://hakin9.org/

Madrid Molina, J. M. (2006). Seguridad en redes inalámbricas 802.11. *Sistemas Y Telemática*, (3), 13–28. Retrieved from

http://bibliotecadigital.icesi.edu.co/biblioteca_digital/handle/10906/400

Rajotiya, D. R. N., & Arora, P. (2012). Enhancing Security of Wi-Fi Network. *International Journal of Computer Application*, *3*(2), 233–239. Retrieved from http://rspublication.com/ijca/JUNE12/22.pdf

Schneier, B., Seidel, K., & Vijayakumar, S. (2016). A Worldwide Survey of Encryption Products. *SSRN Electronic Journal*, *2*, 1–23. http://doi.org/10.2139/ssrn.2731160

Wong, S. (2003). The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. *SANS Institute*, (October), 1–9.

Xiong, J., & Jamieson, K. (2010). SecureAngle: Improving Wireless Security Using Angle-of-Arrival Information. *Proceedings of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks - Hotnets '10*, 1–6.