**La evolución de los protocolos de seguridad inalámbrica**

En los primeros días de Internet, toda la comunicación en línea se realizaba a través de cables físicos. No fue hasta mediados de la década de 1980 que las autoridades de los Estados Unidos designaron un espectro de frecuencias de ondas de radio que podía ser utilizado sin licencia, lo que permitió una mayor expansión de Internet.

A finales de la década del 90 y a principios de los años 2000, se desarrollaron tecnologías para enviar y recibir datos a través de señales de radio. En la actualidad, las personas acceden a Internet de forma inalámbrica a través de computadoras portátiles y de escritorio, teléfonos inteligentes y tablets. Además, los dispositivos inteligentes, tales como termostatos, cerraduras de puertas y cámaras de seguridad, también utilizan Internet inalámbrico para comunicarse entre sí y con los servicios en la red.



**Introducción a los protocolos de comunicación inalámbrica**

En la actualidad, muchas personas utilizan el término Wi-Fi para referirse a Internet inalámbrico. El **Wi-Fi** hace referencia a un conjunto de estándares que definen la comunicación para las redes LAN inalámbricas. El término Wi-Fi fue acuñado como parte de una estrategia  de marketing  por la Wireless Ethernet Compatibility Alliance (WECA), que luego cambió su nombre a Wi-Fi Alliance.

Los estándares y protocolos de Wi-Fi están basados en la familia de estándares de comunicación de Internet 802.11 establecidos por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Por lo tanto, como analista de seguridad, también es posible que veas que el término IEEE 802.11 es utilizado para referirse al Wi-Fi.

Las comunicaciones Wi-Fi están protegidas por protocolos de redes inalámbricas. Estos han evolucionado con el tiempo, ayudando a identificar y resolver vulnerabilidades con tecnologías más avanzadas.

En esta lectura, aprenderás sobre la evolución de los protocolos de seguridad inalámbrica, desde privacidad equivalente por cable (WEP) hasta acceso Wi-Fi protegido (WPA), WPA2 y WPA3. También, conocerás cómo se utilizó el protocolo de aplicación inalámbrica para las comunicaciones de Internet móvil.

**Privacidad equivalente por cable**

La privacidad equivalente por cable (WEP) es un protocolo de seguridad inalámbrico diseñado para proporcionar a los/las usuarios/as el mismo nivel de privacidad en las conexiones de red inalámbrica, que el que tienen en las que son por cable. El protocolo WEP fue desarrollado en 1999 y es el más antiguo de los estándares de seguridad inalámbrica.

Aunque se encuentra en desuso, es recomendable que lo conozcas en caso de que, como analista de seguridad, te encuentres con uno. Puede suceder que un enrutador haya usado WEP como protocolo de seguridad predeterminado y que quien administra la red nunca lo haya cambiado. O bien, puede ocurrir que los dispositivos en una red sean demasiado antiguos como para admitir protocolos de seguridad Wi-Fi más nuevos. Sin embargo, un agente de amenaza podría romper el cifrado WEP, por lo que ahora se considera un protocolo de seguridad muy riesgoso.

**Acceso Wi-Fi protegido**

El acceso Wi-Fi protegido (WPA) fue desarrollado en 2003 para mejorar la privacidad equivalente por cable (WEP), abordar los problemas de seguridad que presentaba y reemplazarla. El WPA estaba pensado como una medida de transición para poder establecer la compatibilidad con hardware más antiguo.

Las fallas de la WEP residían en el propio protocolo y en cómo utilizaba el cifrado. El WPA abordó esta debilidad utilizando el llamado Temporal Key Integrity Protocol (TKIP o también conocido como hashing de clave WEP WPA). El algoritmo de cifrado del WPA utiliza claves secretas más extensas que las del protocolo WEP, lo que dificulta adivinar la clave mediante prueba y error.

El WPA también incluye una verificación de integridad de mensajes que agrega una etiqueta de autenticación con cada transmisión. Si un agente de amenaza intenta alterar la transmisión de alguna manera o reenviarla en otro momento, la verificación de integridad de mensajes de WPA identificará el ataque y rechazará la transmisión.

A pesar de las mejoras de seguridad del WPA, este todavía presenta vulnerabilidades. Los agentes de amenaza pueden valerse de un ataque de reinstalación de clave (o ataque KRACK) para descifrar transmisiones que utilizan WPA. Los atacantes pueden insertarse en el proceso de autenticación del WPA e introducir una nueva contraseña de cifrado en lugar de la dinámica asignada por el WPA. Al configurar la nueva clave como todos ceros, es como si la transmisión no estuviera cifrada en absoluto.

Debido a esta importante vulnerabilidad, el WPA fue reemplazado por una versión actualizada  llamada WPA2.

**WPA2 y WPA3**

**WPA2**

La segunda versión del acceso Wi-Fi protegido (WPA), conocida como WPA2, se lanzó en 2004. El WPA2 es una mejora con respecto al WPA que se basa en el uso del Advanced Encryption Standard (AES). También, optimiza el uso del TKIP. El WPA2 usa Counter Mode Cipher Block Chain Message Authentication Code Protocol (CCMP), que proporciona encapsulación y garantiza la autenticación e integridad de los mensajes. Debido a la fortaleza del WPA2, se considera el estándar de seguridad para todas las transmisiones Wi-Fi en la actualidad. Sin embargo, al igual que su predecesor, el WPA2 es vulnerable a los ataques KRACK. Esto llevó al desarrollo de WPA3 en 2018.

**Personal**

El modo personal del WPA2 es el más adecuado para redes domésticas por diversas razones; es fácil de implementar y la configuración inicial lleva menos tiempo que para la versión empresarial. La frase de contraseña global para la versión personal del WPA2 debe aplicarse a cada computadora y punto de acceso individual en una red. Esto lo hace ideal para redes domésticas, pero poco práctico de gestionar en las organizaciones.

**Empresarial**

El modo empresarial del WPA2 es el más adecuado para aplicaciones corporativas. Proporciona la seguridad necesaria para las redes inalámbricas en entornos comerciales. Si bien la configuración inicial es más complicada que en el modo personal WPA2, el empresarial ofrece un control individualizado y centralizado sobre el acceso Wi-Fi a una red empresarial. Esto significa que quienes administren la red pueden otorgar o eliminar el acceso de los/las usuarios/as a una red en cualquier momento. Los/las usuarios/as nunca tienen acceso a las claves de cifrado, lo que evita que posibles atacantes recuperen las claves de red en computadoras individuales.

**WPA3**

El WPA3 es un protocolo de Wi-Fi seguro y su uso está creciendo a medida que se lanzan más dispositivos compatibles con este protocolo. Las principales diferencias entre el WPA2 y el WPA3 son:

* El WPA3 aborda la vulnerabilidad de intercambio de autenticación a los ataques KRACK, que está presente en el WPA2.
* El WPA3 utiliza la Autenticación Simultánea de Iguales (SAE, por sus siglas en inglés), un acuerdo de autenticación de contraseña y cifrado de claves. Esto evita que los atacantes descarguen datos de las conexiones de redes inalámbricas para intentar descifrarlos.
* El WPA3 incrementó el cifrado para hacer que las contraseñas sean más seguras mediante el uso de encriptación de 128 bits, mientras que el modo WPA3 empresarial ofrece un cifrado opcional de 192 bits.

**Conclusiones clave**

Como analista de seguridad, conocer la historia de cómo se desarrollaron los protocolos de seguridad Wi-Fi te ayudará a comprender mejor qué considerar al proteger redes inalámbricas. Es importante que comprendas las vulnerabilidades de cada protocolo y la importancia de que los dispositivos de tu red utilicen las últimas tecnologías de seguridad.

Marcar como completo