Journal **TechInnovation**
Volumen 3, Número 1, 2024
Universidad Estatal del Sur de Manabí
ISSN-e: 2953-6472

ARTÍCULO ORIGINAL

La seguridad de la red wlan y su evolución en el siglo XXI

Wlan network security and its evolution in the 21st century

https://doi.org/10.47230/Journal.TechInnovation.v3.n1.2024.35-46

Recibido: 14-02-2024 **Aceptado:** 07-04-2024 **Publicado:** 01-06-2024

Belkis Chiquinquirá Cañizales Perdomo[1]*
http://orcid.org/0000-0001-9063-2295

1. Magíster Scientiarum en Gerencia de Empresas Mención: Gerencia de Operaciones; Ingeniera Electricista; Docente de la Carrera de Ingeniería Civil, Facultad de Ciencias Matemáticas y Física; Universidad de Guayaquil; Guayaquil, Ecuador.

Volumen: 3
Número: 1
Año: 2024
Paginación: 35-46
URL: https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/71
***Correspondencia autor:** belkis.canizalesp@ug.edu.ec

RESUMEN

Este estudio da a conocer el aporte de la red WLAN al mundo de la informática, esta es una herramienta práctica y sencilla que permite el manejo de grandes cantidades de datos, al interconectar diferentes equipos tecnológicos, en la actualidad esta red es utilizada en empresas que optan por un sistema digital. El objetivo fundamental de esta investigación es brindar información levante sobre la seguridad en la red WLAN, añadiendo importancia de la protección de las misma. Varias investigaciones demuestran que un gran uso de esta red en dispositivos logrando una excelente conexión. Se aplico una metodología con métodos del nivel empírico y teórico contribuyendo al desarrollo del estudio. Los resultados demostraron la importancia de la red antes mencionada para el desarrollo en las empresas, aunque aún existe desconocimiento sobre los beneficios que esta aporta.

Palabras clave: Conectividad, Datos, Red WLAN.

ABSTRACT

This study reveals the contribution of the WLAN network to the world of computing, this is a practical and simple tool that allows the management of large amounts of data, by interconnecting different technological equipment, currently this network is used in companies that They opt for a digital system. The fundamental objective of this research is to provide relevant information about security in the WLAN network, adding importance to their protection. Several investigations show that great use of this network in devices achieves an excellent connection. A methodology is applied with empirical and theoretical level methods contributing to the development of the study. The results demonstrated the importance of the aforementioned network for the development of companies, although there is still a lack of knowledge about the benefits it provides.

Keywords: Connectivity, Data, WLAN network.

Creative Commons Attribution 4.0 International (CC BY 4.0)

Introducción

En el siglo XXI, la proliferación de redes inalámbricas de área local (WLAN) ha transformado radicalmente la forma en que nos comunicamos, trabajamos y vivimos. Estas redes, que permiten la conexión sin cables a través de tecnologías como Wi-Fi, han facilitado una conectividad ubicua y han impulsado el desarrollo de la economía digital. Sin embargo, este avance tecnológico también ha traído consigo numerosos desafíos en materia de seguridad, convirtiéndose en un campo de interés crucial tanto a nivel internacional, nacional como regional.

Las amenazas a la seguridad de las redes WLAN, a nivel internacional, han crecido exponencialmente. El cibercrimen se ha globalizado, con actores maliciosos que aprovechan vulnerabilidades en las infraestructuras inalámbricas para llevar a cabo ataques sofisticados. Organismos como la Unión Internacional de Telecomunicaciones (UIT) y el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) han trabajado arduamente en el desarrollo y actualización de estándares de seguridad, tales como WPA2 y WPA3, con el objetivo de fortalecer la protección de los datos que circulan a través de estas redes.

En el ámbito nacional, los gobiernos han implementado políticas y normativas específicas para asegurar la integridad y la confidencialidad de las comunicaciones inalámbricas. En muchos países, la legislación sobre protección de datos y ciberseguridad incluye directrices para la gestión segura de las redes WLAN en instituciones públicas y privadas. Por ejemplo, en Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST) ha publicado una serie de recomendaciones y pautas de buenas prácticas para la seguridad de las redes inalámbricas.

Las particularidades geográficas, económicas y culturales a nivel regional, influyen en la adopción y adaptación de medidas de seguridad. En regiones con menor infraestructura tecnológica, las redes WLAN pueden ser más vulnerables debido a la falta de recursos para implementar medidas de seguridad avanzadas. Sin embargo, en regiones con una alta densidad de dispositivos conectados, como las grandes ciudades, se observa una creciente adopción de tecnologías de encriptación y autenticación robustas.

La importancia de investigar la evolución de la seguridad en las redes WLAN radica en la necesidad de proteger la información sensible que se transmite diariamente, prevenir accesos no autorizados y salvaguardar la privacidad de los usuarios. Además, una comprensión profunda de las amenazas y las soluciones emergentes permite desarrollar estrategias proactivas para mitigar riesgos y fomentar un entorno digital seguro.

El objetivo de esta investigación es analizar de manera exhaustiva la evolución de la seguridad en las redes WLAN desde sus inicios hasta la actualidad, evaluando las tecnologías y estándares implementados, las políticas y normativas vigentes, así como las estrategias adoptadas a nivel internacional, nacional y regional. Asimismo, se busca identificar las principales amenazas y vulnerabilidades, y proponer recomendaciones basadas en las mejores prácticas para mejorar la seguridad de las redes WLAN en el futuro.

1. Evolución de las Tecnologías y Estándares de Seguridad en Redes WLAN

Desde la introducción de las primeras redes WLAN, la tecnología ha evolucionado significativamente para mejorar la seguridad de las comunicaciones inalámbricas. Los estándares IEEE 802.11 han sido fundamentales en este progreso.

1.1. WEP (Wired Equivalent Privacy)

Lanzado en 1997, WEP fue el primer estándar de seguridad para redes Wi-Fi. Utilizaba cifrado RC4 para proteger los datos, pero presentaba serias vulnerabilidades debido a sus claves estáticas y al uso de un vector de inicialización (IV) corto. Estas deficiencias permitieron que atacantes pu-

dieran romper la encriptación con relativa facilidad, lo que llevó a la necesidad de desarrollar estándares más seguros.

1.2. WPA (Wi-Fi Protected Access) Introducido en 2003 como una solución temporal a las debilidades de WEP, WPA utilizó el protocolo TKIP (Temporal Key Integrity Protocol) para mejorar la seguridad. Sin embargo, WPA aún tenía limitaciones y vulnerabilidades, lo que impulsó el desarrollo de una versión más robusta.

1.3. WPA2 En 2004, WPA2 se convirtió en el estándar obligatorio para todas las certificaciones de Wi-Fi. Basado en el protocolo de encriptación AES (Advanced Encryption Standard) y el uso del protocolo CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), WPA2 ofreció una seguridad significativamente mejorada. A pesar de ello, también se encontraron vulnerabilidades, como el ataque KRACK (Key Reinstallation AttaCK) descubierto en 2017.

1.4. WPA3 Lanzado en 2018, WPA3 aborda muchas de las deficiencias de sus predecesores, proporcionando una seguridad más fuerte a través de una autenticación más robusta y cifrado individualizado de datos. Incluye características como Simultaneous Authentication of Equals (SAE) para proteger las contraseñas incluso si se utilizan claves débiles.

2. Políticas y Normativas Nacionales

Los gobiernos han jugado un papel crucial en la promoción de la seguridad de las redes WLAN a través de políticas y normativas específicas.

2.1. Estados Unidos El Instituto Nacional de Estándares y Tecnología (NIST) ha desarrollado una serie de guías y estándares, como el NIST Special Publication 800-153, que proporciona recomendaciones sobre la implementación segura de redes WLAN en organizaciones gubernamentales y privadas. Estas pautas incluyen la gestión de claves, autenticación robusta, y monitoreo continuo de la red.

2.2. Unión Europea La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha publicado diversos informes y directrices sobre la seguridad de las redes WLAN, enfocándose en la protección de infraestructuras críticas y la privacidad de los ciudadanos. La normativa GDPR también impone estrictos requisitos sobre la seguridad de los datos personales, afectando directamente la gestión de redes WLAN.

2.3. Asia-Pacífico Países como Japón y Corea del Sur han implementado regulaciones avanzadas en ciberseguridad, con enfoques específicos para la seguridad de las redes inalámbricas. Estas políticas fomentan la investigación y el desarrollo de nuevas tecnologías para proteger las comunicaciones.

3. Estrategias Regionales de Seguridad

Las estrategias de seguridad de las redes WLAN varían significativamente entre diferentes regiones, influenciadas por factores económicos, tecnológicos y culturales.

3.1. América Latina En muchos países de América Latina, la implementación de redes WLAN ha sido un desafío debido a limitaciones económicas y tecnológicas. Sin embargo, ha habido esfuerzos significativos para mejorar la seguridad a través de iniciativas gubernamentales y colaboración internacional. Programas de capacitación en ciberseguridad y la adopción de mejores prácticas internacionales son esenciales para fortalecer la seguridad en la región.

3.2. África En África, la infraestructura tecnológica y la conectividad han crecido rápidamente. Sin embargo, la falta de recursos y de concienciación sobre ciberseguridad plantea riesgos considerables. Iniciativas como las de la Unión Africana y colaboraciones con organizaciones globales buscan cerrar la brecha en la seguridad de las redes WLAN mediante el desarrollo de políticas y marcos regulatorios adecuados.

3.3. Europa del Este En esta región, la transición hacia una economía digital ha sido rápida, lo que ha llevado a una mayor necesidad de redes WLAN seguras. La cooperación con la Unión Europea y la adopción de normativas estrictas han sido claves para mejorar la seguridad en esta área.

4. Principales Amenazas y Vulnerabilidades

Las redes WLAN enfrentan una variedad de amenazas y vulnerabilidades que evolucionan constantemente.

4.1. Ataques de Intercepción y Eavesdropping Los atacantes pueden interceptar las comunicaciones inalámbricas no cifradas o mal cifradas, accediendo a información sensible.

4.2. Ataques de Ingeniería Social El uso de técnicas de ingeniería social para obtener credenciales de acceso sigue siendo una amenaza significativa. Esto incluye phishing y ataques de fuerza bruta dirigidos a redes WLAN.

4.3. Accesos No Autorizados El acceso no autorizado a redes WLAN puede llevar a la explotación de recursos de red y a ataques más amplios dentro de una organización.

4.4. Vulnerabilidades del Hardware y Software Las debilidades en los dispositivos de red y software asociado pueden ser explotadas por atacantes para comprometer la seguridad de la red WLAN.

5. Recomendaciones y Buenas Prácticas

Para mejorar la seguridad de las redes WLAN, es crucial adoptar un enfoque integral que incluya:

5.1. Implementación de WPA3 Adoptar el estándar WPA3 para todas las redes inalámbricas, asegurando una mayor protección contra ataques conocidos.

5.2. Gestión Eficiente de Claves y Autenticación Utilizar métodos de autenticación robustos, como certificados digitales y autenticación multifactor, y gestionar de manera efectiva las claves de cifrado.

5.3. Educación y Concienciación Fomentar la educación y concienciación sobre ciberseguridad entre usuarios y administradores de red para prevenir ataques basados en la ingeniería social.

5.4. Monitoreo y Auditoría Continuos Establecer sistemas de monitoreo y auditoría continua para detectar y responder rápidamente a incidentes de seguridad.

5.5. Actualización Regular de Firmware y Software Mantener los dispositivos de red actualizados con las últimas versiones de firmware y software para proteger contra vulnerabilidades conocidas.

En resumen, la evolución de la seguridad en las redes WLAN refleja una continua adaptación a un panorama de amenazas en constante cambio. La colaboración internacional, la implementación de normativas robustas y la adopción de buenas prácticas son fundamentales para garantizar la protección de las comunicaciones inalámbricas en el siglo XXI.

Metodología

Se utilizaron métodos de la investigación científica tales como:

Métodos teóricos:

Histórico-lógico: se utilizó para sintetizar los antecedentes con énfasis en la seguridad de la red WLAN.

Inducción- deducción: para determinar limitaciones, insuficiencias, falencias y potencialidades en el dominio de la red WLAN del siglo XXI.

Métodos empíricos:

Observación: permitió la identificación de las cualidades de la característica del comportamiento sobre el tema tratado.

Revisión bibliográfica: Se utilizó en la fase de recopilación de información de libros, revistas de carácter científico, internet, los cuales contienen información del tema para la elaboración del presente estudio.

Resultados

WLAN es una sigla de la lengua inglesa que alude a Wireless Local Área Network, una expresión que puede traducirse como Red de Área Local Inalámbrica. Como la denominación lo señala, una WLAN es una red de tipo local cuyos equipos no necesitan estar vinculados a través de cables para conectarse (Ayón Baque, 2021).

Una red informática formada por unidades ubicadas en un espacio geográfico de dimensiones reducidas. Mientras que las computadoras (ordenadores) que forman parte de una LAN se conectan entre sí o a un router con cables, en una WLAN la conexión se realiza utilizando ondas de radiofrecuencia. Las WLAN suelen posibilitar que los usuarios tengan una amplia movilidad, ya que no dependen de cables o elementos físicos para permanecer en la red. La ausencia de cables también contribuye a mantener un orden o una organización en la oficina o el ambiente en cuestión (Sánchez Yancy & Bolaños Cantillo, 2021).

Ventajas y Desventajas

Ventajas de las redes inalámbricas con respecto a las redes que utilizan cables:

- No existen cables físicos: por lo tanto, no hay cables que se enreden, ni que entorpezcan la transpirabilidad o que molesten estéticamente.
- La instalación de redes inalámbricas suele ser más económica.
- Su instalación también es más sencilla.
- Permiten gran alcance; las redes hogareñas inalámbricas suelen tener hasta 100 metros desde la base transmisora.
- Permite la conexión de gran cantidad de dispositivos móviles. En las redes cableadas mientras más dispositivos haya, más complicado el entramado de cables.
- Posibilidad de conectar nodos a grandes distancias sin cableado, en el caso de las redes inalámbricas corporativas.
- Permiten más libertad en el movimiento de los nodos conectados, algo que puede convertirse en un verdadero problema en las redes cableadas.
- Permite crear una red en áreas complicadas donde, por ejemplo, resulta dificultoso o muy cara conectar cables.
- Permite ampliar una red cableada en caso de redes mixtas (mezclas de inalámbricas con cableadas) (Castañeda, 2016).

Desventajas de las redes inalámbricas

- Son algo más inseguras que las redes cableadas, por eso los organismos de defensa e inteligencia gubernamentales utilizan redes con cables dentro de sus edificios.
- El ancho de banda de las redes inalámbricas es menor que las cableadas; en otras palabras, la velocidad alcanzada por las redes cableadas es mayor.
- Las redes inalámbricas son un poco más inestables que las redes cableadas, pueden verse afectada por otras ondas electromagnéticas o aparatos electrónicos cercanos.
- La señal inalámbrica puede verse afectada e incluso interrumpida por objetos, árboles, paredes, espejos, etc (Castañeda, 2016).

WLAN en casa

Las nuevas innovaciones han pasado de ser un instrumento de recreación doméstica a convertirse en una parte importante en la vida del ser humano, para invertir energía en algo atractivo, sin embargo, en este punto las utilizamos para Transmitir la contabilidad en el hogar, llegar a nuestros balances financieros, alojar fotos e información individual y más circunstancias que pueden causar un problema debido a la posibilidad de que alguien no autorizado obtenga esta información.

La forma más habitual de conexión en los hogares es a través de la conexión inalámbrica o Wi-Fi, un tipo de conexión que nos evita depender de un cable.

Esa es la razón por la que dar y aplicar esfuerzos de seguridad en la WLAN (Red de área local inalámbrica) es algo fundamental en la remota posibilidad de que necesitemos protegernos de posibles interrupciones o robos de datos. Existen varias estrategias y diseños que podemos completar para lograr blindar nuestra conexión y la dimensión ideal de seguridad.

Este aspecto relacionado con la seguridad es extremadamente importante y es algo que se debe considerar en cualquier campo donde funcione un sistema Wi-Fi.

Este tipo de consejos son muy recurrentes, tanto en los medios de comunicación particulares en el campo innovador como en los medios más generalistas, hasta el punto de que podemos leer los consejos coherentes con este punto de vista en El País e incluso en las revistas en línea de Movistar, cada una de ellas planificada, para ayudarnos en las medidas que debemos tomar para evitar cualquier desastre y estar protegidos de cualquier asociación o robo de datos no aprobados.

Dentro de toda la información que nos encontramos, podemos indicar que **unas buenas prácticas en relación a nuestra conexión WLAN son las siguientes:**

- **Actualizar el router a la última versión disponible:** Estas actualizaciones ofrecen parches de seguridad que evitarán la explotación de posibles agujeros
- **Cambiar la configuración por defecto:** Nombre y usuario de acceso al router, el nombre de la red, la contraseña, etc.
- **Hacer uso de cifrado WPA2:** Este método de cifrado es el más seguro hasta la fecha.
- **Hacer uso de una contraseña fortificada:** Cuanto más compleja sea y menos obvia, mejor, de hecho, la mejor solución es mezclar números y letras a lo largo de toda la clave de acceso.
- **Ocultar la red:** De esta forma será más complicado que una persona ajena a nosotros logre localizarla o acceder a ella.
- **Activar el filtrado MAC:** Indicando únicamente nuestros equipos y dispositivos y denegando la conexión a cualquier otro que no sean los indicados.
- **Desactivar el servicio DHCP:** Esta medida no es tan segura, pero nunca está de más, ya que desactivando este servicio será necesario configurar la tarjeta de red con una dirección IP válida y con la dirección IP de la puerta de enlace, es decir, del Router (Guereta, 2018).

No existe dudas de que no hay seguridad total en el campo tecnológico, obviamente podemos decir que al impulsar este tipo de medidas y adquirir datos y documentación particular en páginas o sitios dedicados a ellos, es muy probable que nunca obtengamos un acceso no autorizado a nuestro sistema, por lo que habremos logrado nuestro objetivo de garantizar una buena seguridad a nuestro hogar (Guereta, 2018).

WLAN en la empresa: La conectividad inalámbrica en los entornos laborales era una opción complementaria o una alternativa cuando no era posible la comunicación cableada, pero tanto el tiempo como la evolución de la tecnología y, sobre todo, de las necesidades y exigencias de los usuarios, la conectividad inalámbrica se ha convertido en una prioridad de las empresas.

Las red ofrecen soluciones inalámbricas para empresas, no se trata solo de puntos de acceso, que también son necesarios, o de routers, imprescindibles, igualmente, sino que hablamos, además, de la gestión y de la monitorización y de una serie de servicios que se pueden llegar a implementar sobre

la propia infraestructura de red, como, por ejemplo, la creación de una red inalámbrica para clientes o visitantes que pueda utilizarse como un punto de recopilación de información si la empresa así lo necesita, servicios de marketing, servicios alrededor de vídeo y redes sociales, o, incluso, analítica de los datos que nos proporcione la propia red.

Un punto de arranque importante: una buena planificación: Si hay dos aspectos que diferencian una buena solución de WLAN profesional es la cobertura que ofrece a los empleados que deben usarla y el rendimiento. Y para ambos aspectos es fundamental una adecuada planificación. Como ya hemos señalado, la cobertura inalámbrica resulta imprescindible cada vez para un mayor número de clientes. Pero el avance de la tecnología y el crecimiento en número de los dispositivos (BYOD) y puntos de acceso puede convertir la instalación WLAN en una tarea complicada de planificar, primero, y de gestionar después (itUser, 2016).

La WLAN no solo se usa en un entorno de oficina para el envío de mails o la consulta del tráfico web. Hay otros muchos escenarios a tener en cuenta. Por ejemplo, los comerciantes utilizan lectores de códigos de barras con conexión WLAN integrada para registrar su stock o incluso toda su mercancía, totalmente automatizada, con robots utilizando módulos integrados de WLAN. En estos casos, una buena cobertura resulta imprescindible (itUser, 2016).

Las máquinas transmiten la información sobre el estado de la temperatura, los errores que puedan acontecer o directamente lanzan órdenes de compra generadas automáticamente cuando necesitan nuevas materias primas. En caso de que surgieran problemas que afectasen a la red, es imprescindible informar al administrador lo antes posible. Una red de alta disponibilidad garantiza el buen funcionamiento de todo el proceso. De lo contrario las órdenes no podrían ser enviadas a la máquina, pudiendo quedar fuera de servicio, y esto se traduce en tiempo de espera para el cliente (itUser, 2016).

El alcance de las aplicaciones ha crecido a niveles muy superiores a los tradicionales, y la conexión WLAN se usa para distintas comunicaciones, ya sea de voz, datos o, incluso, vídeo. En estos casos, la velocidad de la red es fundamental, tanto para la voz como para los datos. Las redes de área amplia utilizan un esquema de direccionamiento uniforme porque el envío sin dirección de datos sería ineficiente con el número de redes conectadas. Los sistemas intermedios o nodos de red, como conmutadores, puentes y enrutadores garantizan que los paquetes de datos enviados se reenvían a la dirección correcta. Mediante el hardware, los paquetes de datos se envían de una subred a la otra y se entregan al participante de red correcto, ya sea un PC, un teléfono inteligente, un televisor o un refrigerador (itUser, 2016).

Otro elemento en este de por sí complicado tablero, y es que los usuarios que se conectan a la red no lo hacen solo con un dispositivo, sino que utilizan un número que algunos informes sitúan en, al menos, siete (PC/portátil, smartphone, tableta, smartwatch, cámara…), y con todos ellos quieren la misma experiencia de uso (itUser, 2016).

Existe una nueva área de aplicación WLAN cada vez mayor herramienta de localización en tiempo real (RTLS), algo usado, por ejemplo, en las rondas médicas móviles de los hospitales (itUser, 2016).

A la hora de planificar una infraestructura de red hay que tener en cuenta aspectos tan significativos como el número de clientes (no personas, sino dispositivos) conectados a cada punto de acceso, la ubicación de los mismos dentro del área de la empresa (el área por el que se despliegue al red), ancho de banda que necesitan los clientes (no es lo mismo si van a trabajar con datos, vos o, incluso, vídeo de alta calidad), latencia que necesitan los clientes (dependiendo de

la actividad de cada cliente o empresa, el tiempo de respuesta indicado para la red puede variar de forma significativa), si existen interferencias por otras redes o transmisiones que puedan afectar, o cómo de diáfana o compleja es la superficie a cubrir, por indicar algunos aspectos que hay que tener en cuenta a la hora de realizar una adecuada planificación (itUser, 2016).

Tipos de ataques a redes WLAN: Ataques pasivos: El objetivo del agresor es obtener datos. Son un paso inicial para posteriores asaltos. Unos pocos ejemplos de este tipo son el reconocimiento el espionaje, la escucha sigilosa, el aprendizaje y la revelación de contraseñas.

Los ataques activos Incluyen alterar o hacer flujos de información falsos en la transmisión. Pueden tener dos metas distintas, reemplazar robar identidad o colapsar las administraciones proporcionadas por el sistema (servicios). Unos de los ejemplos de estos ataques son, el establecimiento de puntos de acceso AP no aprobados.

Para evitar estos tipos de ataques es necesario diferentes protocolos que con el paso del tiempo fueron mejorando. Se aclaran y explicaran.

Protocolos de seguridad en redes WLAN: Los protocolos de seguridad que se pueden conectar a los sistemas WLAN son diversos, entre las que se incluyen: seguridad proporcional por cable (WEP), acceso Wi-Fi asegurado a (WPA), IEEE 802.11i y acceso seguro a Wi-Fi2 a (WPA2), a pesar de del hecho de que, además, pueden utilizar diferentes componentes, por ejemplo, obtener registros de control (ACL) que también se aplican a diferentes tipos de sistemas, sin embargo, dado que los sistemas remotos son un aumento de los sistemas cableados, les puede preocupar. En cuanto a las convenciones de seguridad en WLAN organizadas, hay dos puntos de vista cruciales a considerar: la verificación y el cifrado, por lo que este trabajo se concentrará en ellos cuando se construya la correlación. El cifrado es el tratamiento de una gran cantidad de información, contenida o no en un paquete, a fin de evitar que alguien, se beneficie de su comprensión. Normalmente se utiliza un cálculo y una clave de cifrado para esto La confirmación es el camino para verificar y garantizar el carácter de las reuniones asociadas con un intercambio. A través de él, se evita que un elemento cree una personalidad falsa, poniendo en peligro la protección y la confiabilidad de los datos. En la técnica de validación abierta, el gadget del cliente envía un mensaje de solicitud de verificación, al que el AP responde con un mensaje de reacción de confirmación. Cuando se trabaja en este modo, un AP reconoce cualquier solicitud. A pesar del hecho de que, allí es donde se puede completar la separación de MAC (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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 =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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

En la 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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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, 2005) y (Rumale, 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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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 au-

torizados. 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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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, 2005). 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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

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 (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

Protocolos SSL, SSH Y HTTPS: Este tipo de protocolo en redes WLAN abarca caracteres específicos, por ejemplo, SSL, SSH y HTTPS. El protocolo SSL, cuya versión actual es la variante 3.0 en 1996 por el IETF en RFC 6101 es una convención criptográfica destinada a la utilización de correspondencias seguras en Internet. Lo que depende de la utilización de testamentos avanzados y se ha convertido en el verdadero estándar para intercambios web seguros. HTTPS es la variante segura de HTTP que utiliza el cifrado basado en SSL para hacer un canal más adecuado para los datos sensibles al tráfico que la convención HTTP. SSL y HTTPS permiten generar una mayor seguridad a través del acceso web entre el cliente y el servidor, asegurar el procedimiento de confirmación con procesos y la posibilidad de utilizar instrumentos, por ejemplo, firebug, que es un módulo para Firefox, con el que puede ver la información. Movimientos entre clientes y servidores web, el cliente y la clave y contraseñas que se ingresen durante la conexión (González Paz, Beltrán Casanova, & Fuentes Gari, 2016).

Conclusiones

La seguridad de las redes WLAN ha avanzado considerablemente a lo largo del siglo XXI, impulsada por la evolución tecnológica y el desarrollo de políticas y normativas robustas. La adopción de estándares de seguridad más avanzados, junto con estrategias de gestión de seguridad integral y educación en ciberseguridad, ha mejorado significativamente la protección de las redes inalámbricas. Sin embargo, el panorama de amenazas sigue evolucionando, lo que requiere una vigilancia continua y una

adaptación constante de las medidas de seguridad. La cooperación internacional y la implementación de mejores prácticas seguirán siendo cruciales para enfrentar los desafíos futuros y garantizar la seguridad de las comunicaciones inalámbricas en un mundo cada vez más digitalizado.

Bibliografía

Ayón Baque, B. M. (2021). Análisis de los beneficios de la tecnología mesh en las redes inalámbricas del complejo universitario UNESUM. Universidad estatal del sur de Manabí, Facultad de Ciencias Técnicas. Obtenido de https://repositorio.unesum.edu.ec/bitstream/53000/2667/1/AYON%20BAQUE%20BYRON%20MICHEL.pdf

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

Castañeda, L. F. (2016). Estructura de red de Grupo Soluciones Siempre. UNIVERSIDAD POLITÉCNICA DE SINALOA. Obtenido de http://repositorio.upsin.edu.mx/Fragmentos/tesinas/Tesina2152.pdf

González Paz, A., Beltrán Casanova, D., & Fuentes Gari, E. (2016). Propuesta de protocolos de seguridad para la red inalámbrica local de la Universidad de Cienfuegos. Revista Universidad y Sociedad, 8(4), 130-137.

Guereta, T. (20 de 03 de 2018). Obtenido de www.rootear.com: https://rootear.com/seguridad/asegurar-red-wlanitUser. (5 de abril de 2016). Obtenido de https://www.ituser.es/content-marketing/2016/04/wlan-en-la-empresa

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

Rumale, A. &. (2011). IEEE 802.11x, and WEP, EAP,WPA . Obtenido de WPA2.

Sánchez Yancy, D., & Bolaños Cantillo, C. (2021). Diseño y simulación de una red de comunicaciones de conexión punto a multipunto de topología anillo para conectar a tres sedes de la institución educativa departamental Sagrado Corazón de Jesús de Pivijay–Magdalena. Universidad cooperativa de colombia, facultad de ingenieria. Obtenido de https://repository.ucc.edu.co/server/api/core/bitstreams/8e0535e0-8214-4dcf-a520-60d18874e7a8/content

Cómo citar: Cañizales Perdomo, B. C. . (2024). La seguridad de la red wlan y su evolución en el siglo XXI. Journal TechInnovation, 3(1), 35–46. https://doi.org/10.47230/Journal.TechInnovation.v3.n1.2024.35-46