Journal **TechInnovation**
Volumen 2, Número 1, 2023
Universidad Estatal del Sur de Manabí
ISSN-e: 2953-6472

ARTÍCULO DE REVISIÓN

Impacto en la seguridad de las redes inalámbricas

Impact on the security of wireless networks

https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.62-71

Recibido: 04-08-2023 **Aceptado:** 27-06-2023 **Publicado:** 01-06-2023

Julio César Borrero Neninger[1]*
https://orcid.org/0000-0001-9648-772X

Ponce Guerrero José Luis[2]
https://orcid.org/0000-0003-4237-5225

1. Ingeniero en Formación en la carrera de Tecnologías de la Información de la Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
2. Ingeniero en Formación en la carrera de Tecnologías de la Información de la Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
3. Ingeniero en Formación en la carrera de Tecnologías de la Información de la Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.

Volumen: 2
Número: 1
Año: 2023
Paginación: 62-71
URL: https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/43
***Correspondencia autor:** jborrero@uho.edu.cu

RESUMEN

Las redes inalámbricas han revolucionado la forma en que la sociedad se conecta y comunica, lo que ha llevado a un aumento exponencial en la dependencia de la tecnología inalámbrica. La creciente conectividad también ha expuesto a diversos riesgos de seguridad. En el estudio se revisa y analiza los desafíos y avances más relevantes, con un enfoque en el impacto actual que estos aspectos tienen en la protección de datos y la privacidad de los usuarios. El análisis aborda aspectos clave en la seguridad de redes inalámbricas, incluyendo protocolos de seguridad, vulnerabilidades y ataques frecuentes. Se examinan las debilidades comunes en protocolos de encriptación, como WEP y WPA, que han sido objeto de ataques de fuerza bruta y explotación de vulnerabilidades. A su vez, se conoce los protocolos más seguros, como WPA2 y WPA3, que han mejorado significativamente la resistencia a ataques. La aparición de tecnologías emergentes, como el Internet de las Cosas (IoT) y la 5G, ha ampliado el panorama de la seguridad inalámbrica, estas nuevas tecnologías han traído consigo desafíos únicos, como la proliferación de dispositivos IoT inseguros que pueden servir como puntos de entrada para intrusos. Se analizan soluciones basadas en IA que pueden identificar patrones de tráfico malicioso y comportamientos anómalos, lo que contribuye a una respuesta más rápida y eficiente ante incidentes de seguridad. En conclusión, la seguridad de las redes inalámbricas sigue siendo un desafío constante debido a la evolución tecnológica y el aumento de las amenazas cibernéticas.

Palabras clave: Protocolos de seguridad¸ Tecnologías emergentes; Vulnerabilidades.

ABSTRACT

Wireless networks have revolutionized the way society connects and communicates, leading to an exponential increase in reliance on wireless technology. The increasing connectivity has also exposed various security risks. The study reviews and analyzes the most relevant challenges and advances, with a focus on the real impact that these aspects have on data protection and user privacy. The analysis addresses key aspects of wireless network security, including security protocols, vulnerabilities, and frequent attacks. Common weaknesses in encryption protocols, such as WEP and WPA, that have been subjected to brute force attacks and vulnerability exploitation are examined. In turn, it knows the most secure protocols, such as WPA2 and WPA3, which have significantly improved resistance to attacks. The emergence of emerging technologies such as the Internet of Things (IoT) and 5G have broadened the landscape of wireless security, these new technologies have brought with them unique challenges, such as the disappearance of insecure IoT devices that can serve as access points. entrance for intruders. AI-based solutions that can identify malicious traffic patterns and anomalous behaviors are discussed, contributing to faster and more efficient response to security incidents. In conclusion, the security of wireless networks continues to be a constant challenge due to technological evolution and the increase in cyber threats.

Keywords: security protocols¸ emerging technologies; vulnerabilities.

Introducción

El estudio aborda las implicaciones de la seguridad en entornos empresariales y de usuarios domésticos. Se discuten las mejores prácticas de seguridad, como el uso de autenticación de dos factores y la segmentación de redes, para mitigar riesgos y mejorar la protección. Asimismo, se explora el papel de la inteligencia artificial y el aprendizaje automático en la detección y prevención de ataques en redes inalámbricas.

WLAN es una amplia red inalámbrica que permite conectar un equipo a la red para acceder a Internet, impresoras y demás servicios sin necesidad de cables. Probablemente la desventaja más grande de las conexiones inalámbricas es que es de fácil acceso para los hackers detectar estas señales y obtener su información privada. La transferencia de datos confidenciales sobre una conexión inalámbrica plantea graves riesgos a su identidad como es su información personal, tales como números de tarjetas de crédito y datos bancarios. En la actualidad el tema de la seguridad inalámbrica es en el que más hincapié se está haciendo. El nivel de seguridad actual de estas redes está a años luz del de sus comienzos. Al ser el aire el medio de propagación empleado por las ondas hace que la información esté expuesta a sufrir distintos tipos de ataques, por lo que es el inconveniente más importante que presentan las WLAN en cuanto a seguridad (Ramírez, Polanco y Farías s.f.).

Las redes inalámbricas, por la gran movilidad que aportan, se han convertido en un sector de acelerado crecimiento en las comunicaciones. La aspiración del hombre de llevar información cada vez más lejos sin necesidad de cables, la comodidad en la conexión y el rápido despliegue que representan son algunos de los aspectos que motivan su rápida asimilación (Ocampo 2018).

La evolución de las amenazas en redes inalámbricas se ha observado en el crecimiento acelerado de la tecnología inalámbrica, esto ha ido acompañado de una evolución igualmente rápida de las amenazas en materia de seguridad. Las redes inalámbricas han pasado de ser utilizadas principalmente en entornos domésticos al ser fundamentales en infraestructuras críticas, empresas, instituciones educativas y más. Todo lo anterior, ha atraído la atención de ciberdelincuentes que buscan explotar vulnerabilidades en estas redes para acceder a información sensible, comprometer la privacidad de los usuarios o interrumpir servicios vitales. La amplia disponibilidad de herramientas y técnicas de hacking ha hecho que la seguridad de las redes inalámbricas sea más desafiante que nunca.

Los protocolos de seguridad en redes inalámbricas son elementos esenciales para proteger la confidencialidad e integridad de los datos transmitidos. Sin embargo, algunos de los protocolos más antiguos, como el Wired Equivalent Privacy (WEP), han demostrado ser altamente vulnerables a ataques y su uso se ha desalentado ampliamente. Aunque los protocolos más recientes, como el Wi-Fi Protected Access (WPA2) y WPA3, ofrecen mejoras significativas en seguridad, aún enfrentan desafíos y debilidades que los ciberdelincuentes buscan explotar. El desarrollo y la adopción de protocolos de seguridad más sólidos y resistentes a los ataques continúan siendo un área de investigación y desarrollo crucial en la seguridad de redes inalámbricas.

La amenaza del Internet de las Cosas (IoT), la proliferación de dispositivos conectados en el Internet de las Cosas (IoT) ha agregado una capa adicional de complejidad a la seguridad de las redes inalámbricas. Muchos de estos dispositivos IoT carecen de medidas de seguridad adecuadas y representan puntos débiles potenciales en la red. Los ataques dirigidos a dispositivos IoT, como cámaras de seguridad, electrodomésticos inteligentes o sensores, pueden comprometer la privacidad de los usuarios y facilitar el acceso no autorizado a la red.

La segmentación de redes y la aplicación de políticas de seguridad específicas para los dispositivos IoT se han vuelto esenciales para mitigar este riesgo.

La revolución de la 5G y sus implicaciones de seguridad, así como la adopción generalizada de la tecnología 5G ha brindado beneficios significativos en términos de velocidad y capacidad de las redes inalámbricas. Sin embargo, la 5G también ha introducido nuevos desafíos de seguridad. La virtualización y la compartición de recursos en arquitecturas 5G pueden abrir nuevas superficies de ataque, y los desafíos de autenticación y privacidad asociados con esta tecnología deben ser abordados adecuadamente. La implementación de soluciones de seguridad adaptadas a las redes 5G es crucial para garantizar que la promesa de esta tecnología no se vea empañada por problemas de seguridad.

El uso de inteligencia artificial (IA) y aprendizaje automático en la seguridad de redes inalámbricas ha ganado impulso significativo en los últimos años. Las capacidades de la IA para analizar patrones de tráfico, detectar comportamientos anómalos y responder en tiempo real a amenazas potenciales ofrecen una ventaja importante en la lucha contra los ataques cibernéticos. La adopción de soluciones de IA en la seguridad de redes inalámbricas está en constante evolución y promete mejorar significativamente la resiliencia de estas redes ante las amenazas emergentes.

El impacto de la seguridad en las redes inalámbricas es un tema crítico en un mundo cada vez más conectado. La evolución de las amenazas, los protocolos de seguridad, el auge del IoT, la adopción de la 5G y el papel de la IA en la detección de amenazas, todos contribuyen a un escenario en constante cambio. Abordar estos desafíos con enfoques proactivos y soluciones innovadoras es fundamental para proteger la integridad y la privacidad de las redes inalámbricas en la actualidad y en el futuro.

Por otro lado, se puede decir que la seguridad en ocasiones ha quedado vulnerables a diversos tipos de ataques. Aunque es muy común asociar el término "redes inalámbricas" a las redes conocidas como WiFi, en la actualidad esta familia incluye muchas otras tecnologías. Es posible encontrar tecnologías que se mueven entre tres grupos distintos. El primero se denomina redes WWAN (Wireless Wide Area NetworkRedes Inalámbricas de Área Amplia) cuya potencia y alcance permiten abarcar grandes espacios e incluso ciudades.

Las redes inalámbricas cuentan con numerosos mecanismos y protocolos que aunque no garantizan de forma absoluta la integridad y confidencialidad de la información que por ellas transita, sí proporcionan barreras que reducen de forma considerable la cantidad de personas capaces (por sus conocimientos y recursos) de efectuar ataques exitosos que llegan al punto de competir con muchas de las soluciones cableadas actualmente disponibles.

En cuanto a las redes de área personal (WPAN), la situación con respecto a la seguridad no ha despertado gran alarma, si se tiene en cuenta fundamentalmente el corto alcance que permiten y su baja aplicación en redes locales. Mecanismos de seguridad Existen varios mecanismos creados para ofrecer seguridad a estas redes. Entre los más conocidos se ubican los protocolos de encriptación de datos WEP y el WPA para los estándares 802.11, que se encargan de codificar la información transmitida para proteger su confidencialidad. Dichos estándares son proporcionados por los propios dispositivos inalámbricos.

Protocolos de seguridad

Wired Equivalent Privacy (WEP): fue uno de los primeros protocolos de seguridad diseñados para proteger las redes inalámbricas. Sin embargo, ha sido ampliamente considerado como inseguro debido a sus debilida-

des criptográficas. Los ataques de fuerza bruta y la fácil recuperación de la clave de cifrado han hecho que WEP sea vulnerable y se desaconseje su uso en entornos modernos (ciberriesgos.com 2023).

Wi-Fi Protected Access (WPA): Para abordar las debilidades de WEP, se introdujo WPA como una mejora significativa. WPA utiliza el algoritmo de cifrado TKIP (Temporal Key Integrity Protocol) para generar claves únicas para cada paquete de datos transmitido. Esto proporciona un nivel más alto de seguridad en comparación con WEP. Sin embargo, a medida que la tecnología avanzaba, también se descubrieron vulnerabilidades en WPA.

Wi-Fi Protected Access 2 (WPA2): es actualmente el protocolo de seguridad más ampliamente utilizado en redes inalámbricas. Utiliza el algoritmo de cifrado AES (Advanced Encryption Standard) en lugar de TKIP, lo que proporciona un nivel de seguridad mucho más sólido. Aunque WPA2 ha demostrado ser resistente a muchos ataques, aún enfrenta desafíos, como el ataque de diccionario para contraseñas débiles.

Wi-Fi Protected Access 3 (WPA3): es la versión más reciente y mejorada de los protocolos de seguridad para redes inalámbricas. Introduce mejoras significativas en la autenticación y cifrado. WPA3 emplea el protocolo de establecimiento de clave de simulación de autenticación (SAE) para proteger las contraseñas contra ataques de fuerza bruta. También proporciona una mayor protección en entornos públicos mediante el cifrado individual de datos para cada dispositivo conectado.

Extensible Authentication Protocol (EAP): el protocolo EAP no es en sí mismo un protocolo de cifrado, sino más bien un marco de autenticación utilizado en combinación con otros protocolos, como WPA2 y WPA3. EAP permite una amplia variedad de métodos de autenticación, como EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security), y PEAP (Protected EAP), lo que permite un enfoque más flexible y seguro para la autenticación en redes inalámbricas.

Es esencial entender que la elección del protocolo de seguridad adecuado depende de la infraestructura y los requisitos específicos de cada red inalámbrica. Para garantizar la máxima seguridad, es fundamental mantener los dispositivos actualizados con las últimas actualizaciones de firmware y configurar contraseñas sólidas y únicas para evitar el acceso no autorizado. La seguridad de las redes inalámbricas es una responsabilidad continua y debe ser una prioridad para todos aquellos que implementan y mantienen estas infraestructuras.

Violación de Filtrado de Protocolo

Esta regla de seguridad es más difícil de violar, generalmente los ataques de este tipo están orientados al protocolo seguro permitido (casi nunca tan seguro como se dice). Por desgracia de los administradores y para bien de los atacantes, muy pocos dispositivos implementan filtrados de protocolos potentes y los que lo hacen tienen elevados costos (EcuRed 2023).

Violación del Protocolo WEP

Es el más antiguo para la seguridad de las redes inalámbricas y aun altamente utilizado como mecanismo de seguridad primario. Contra este protocolo se pueden realizar ataques de fuerza bruta, de FMS o ataques FMS mejorados, todos encaminados a violentar el algoritmo RC4 para obtener la clave WEP. Asegurando la red inalámbrica (EcuRed 2023).

Principios generales que pueden ser aplicados para elevar el nivel defensivo

Las redes inalámbricas sí pueden ser bastante seguras. Toda red puede ser violada,

es cierto, pero la seguridad no se basa en la impenetrabilidad, sino en lograr que el punto de ruptura se alcance por muy pocas personas en el mundo, si existe alguna (EcuRed 2023).

La clave del éxito

Crear una política de seguridad inalámbrica. Lo primero para la implementación de una red inalámbrica es desarrollar una adecuada política de acceso. Una red será tan segura como lo sea su miembro más vulnerable, es decir, cada equipo debe ser capaz de soportar la variante de seguridad que usted elija. Si se emplean filtros MAC, la base de datos con todos los clientes MAC debe ser actualizada y verificada a intervalos. O sea, debe llevarse la red a un estado de igualdad que garantice el mismo nivel de seguridad en todas las estaciones. Los usuarios, como principal elemento en la política de seguridad, deben ser educados y formar parte proactiva de dicha seguridad, de forma que ante hechos como por ejemplo la pérdida de un equipo, lo reporten para que se tomen las medidas de exclusión de la red de dicho equipo. Estos deben poseer una adecuada seguridad física que imposibilite su hurto o daño. Los custodios deberán informar sobre cualquier equipo inalámbrico que aparezca y genere una amenaza potencial de ataque. Deben utilizarse potencias adecuadas de transmisión para evitar la radiación a áreas donde no se requiera el uso de la red inalámbrica. La utilización de varios puntos de acceso incrementa el riesgo del ataque tipo "maninthemiddle" (hombre en el medio). Para evitarlo deben utilizarse diferentes dominios para la red cableada. Si por necesidad varios puntos de acceso estuviesen conectados a un mismo switch, deberán emplearse VLANs y colocar en una misma VLAN todos los puntos de acceso si es posible. Los identificadores de red ESSIDs no deberán aportar ninguna información que revele el más mínimo detalle sobre la red (danielbenvenuto.com 2023).

Los protocolos de seguridad utilizados, si son propietarios como alguna mejora del WEP, por ejemplo, deben ser certificados por auditores de seguridad externos. Debe garantizarse una adecuada política de selección de contraseñas y evitarse a toda costa el uso de protocolos no necesarios, así como el empleo de recursos compartidos. La red inalámbrica debe ser monitorizada y comparada contra un comportamiento habitual. Las desviaciones de este comportamiento han de estar documentadas. El despliegue de detectores de intrusos debe ser realizado, así como el análisis de las alarmas que éstos puedan generar. Claro, no puede faltar en la política, la existencia de un equipo de respuestas a las incidencias que esté familiarizado con las regulaciones locales para el manejo de las evidencias. Redes VPN en las capas altas de la red inalámbrica Al hacer un análisis del propio nombre VPN (Virtual Private Network) se obtienen tres elementos que de por sí definen su función. El primero Virtual, indica la coexistencia pacífica de dos redes mutuamente excluyen tes en un mismo segmento de red (danielbenvenuto.com 2023).

La segunda parte Prívate (privada) indica una forma de comunicación que es solamente entendible por los extremos que participan en ésta, mientras que la tercera Network (red) se explica por sí sola. Las redes privadas virtuales son una excelente solución sobre las inalámbricas que están llenas de usuarios "imprevistos" y poblando las bandas libres. Este tipo de red se utiliza sobre medios cableados fundamentalmente para trabajadores a distancia u oficinas alejadas de la empresa, en el mundo sin cables se puede aplicar a cualquier enlace que se desee proteger. Existen apuestas sobre el futuro estándar 802.11i (WPA2) y la reducción que traerá en la implementación de VPNs inalámbricas, pero quizás como dice el refrán "más vale malo conocido que bueno por conocer". Antes que se publicara el borrador final del 802.11i ya existían considerables problemas relativos a su se-

guridad. De seguro estos problemas se irán solucionando e irán apareciendo nuevos que serán objeto de nuevos ataques. Por consiguiente, los gestores de red preferirán los mecanismos de seguridad ya conocidos y probados como una VPN con IPSec. Sistemas IDS Inalámbricos (danielbenvenuto.com 2023).

Sistemas de detección de intrusos

Los sistemas de detección de intrusos (IDS, siglas en inglés) se agrupan en dos categorías: basados en firmas y basados en conocimientos. Los primeros asientan su funcionamiento en analizar y comparar los eventos de la red con firmas conocidas de ataques que poseen en una base de datos. Son de fácil implementación, pero también son más fáciles de violar, sin tomar en cuenta que las bases de firmas tienen que estar protegidas. Este tipo de sistema es poco probable que detecte violaciones novedosas. Por otra parte, los sistemas basados en conocimiento fundan su existencia en analizar y describir el funcionamiento estadístico de la red, avisando de comportamientos que se desvíen de esta media. Lo malo es que pueden generar falsos positivos, sobre todo en un medio como el inalámbrico debido a su naturaleza no fiable. Además, no hay garantías de que el análisis de la red se haya comenzado cuando ya estuviera siendo atacada por un intruso. Un sistema IDS inalámbrico debe pertenecer a ambas categorías, pues son pocas las herramientas de ataque inalámbrico que poseen firmas conocidas, mientras la mayoría sólo produce pequeñas desviaciones del comportamiento habitual. Es digno considerar que equipos cercanos a nuestra WLAN que operen en las bandas libres, como puede ser un horno microondas, genere "malformaciones" en los paquetes de datos de nuestra red y dichos paquetes sean interpretados por el IDS como ataques. En ese caso el atacante será un malvado horno microondas, mientras cocina unas deliciosas palomitas de maíz. Por esto la clave para un despliegue eficiente de una red WLAN es caracterizar detalladamente su funcionamiento durante un tiempo significativo. Sólo recogiendo un gran número de estadísticas sobre el comportamiento de la red se podrá determinar si un proceder es anómalo o no (danielbenvenuto.com 2023).

En el mercado actual no existen herramientas que clasifiquen en los dos grupos antes mencionados. Es cierto que existen soluciones que buscan MAC y valores ESSID ilegales en la red, pero suelen ser una pérdida de tiempo y dinero. Es de especial interés para usuarios y administradores valorar los riesgos asociados a la instalación de este tipo de tecnologías y tomar las medidas necesarias para combatirlos, medidas que muchas veces no son tan costosas o complicadas. Especial atención debe observarse en los enlaces de largo alcance, pues hay tecnologías como 802.11 con antenas bien diseñadas para estos fines y 802.16 pueden alcanzar distancias en el orden de 10 kilómetros o más en el caso de WiMax. En nuestro país han comenzado a surgir muchos enlaces de este tipo, algunos de los cuales utilizan WEP en el mejor de los casos. Como se ha dicho, si bien es imposible crear mecanismos infalibles, sí se puede obstaculizar en forma considerable la penetración de intrusos implementando soluciones serias WPA y VPNs en capas altas, al mismo tiempo se recomienda comprobar los niveles de seguridad, ejecutando ataques de prueba sobre nuestras redes (EcuRed 2023).

Metodología

Se realizo una revisión bibliográfica del estado del arte, en esta etapa se conoció la literatura científica y técnica relacionada con la seguridad de las redes inalámbricas. Se recopilaron y analizaron investigaciones previas, artículos científicos, informes técnicos y fuentes confiables que aborden temas como la evolución de las amenazas,

los protocolos de seguridad utilizados y los desafíos actuales en el contexto del Internet de las Cosas y la tecnología 5G. Esta revisión permitió establecer una base sólida para el estudio y identificar las áreas clave de investigación.

Definición de objetivos e hipótesis, con el método hipotético-deductivo: se establecieron los objetivos específicos de la investigación y se formularon las hipótesis sobre la eficacia de los protocolos de seguridad actuales, identificando las vulnerabilidades comunes en las redes inalámbricas y el impacto de la tecnología 5G en la seguridad de estas redes.

El estudio tuvo un enfoque cualitativo metodológico, para alcanzar los objetivos planteados a través del análisis de datos, simulaciones y combinaciones de métodos.

Recopilación de datos: En esta etapa, se recopilarán los datos necesarios para llevar a cabo el estudio. Esto podría implicar la realización de pruebas de seguridad en entornos controlados o la recolección de datos de redes inalámbricas reales. También se podrían utilizar herramientas de análisis de tráfico o software de simulación para generar datos relevantes.

Análisis-síntesis: se procedió con el análisis de datos, así como el procesamiento de la información recolectada para responder a las preguntas de investigación y verificar las hipótesis planteadas. Se pueden utilizar técnicas estadísticas, visualizaciones de datos y otras herramientas de análisis para extraer conclusiones significativas.

La metodología descrita proporcionó una base sólida para abordar el tema del impacto en la seguridad de las redes inalámbricas de manera sistemática

Resultados

El impacto en la seguridad de las redes inalámbricas, se conoció a través de varios aspectos clave relacionados con la seguridad de estas redes, incluidos los protocolos de seguridad utilizados, las amenazas emergentes, las implicaciones de la tecnología 5G y el papel de la inteligencia artificial en la detección y prevención de amenazas.

En cuanto a los protocolos de seguridad, se encontró que los protocolos más antiguos, como Wired Equivalent Privacy (WEP), son altamente vulnerables y no proporcionan una protección adecuada para las redes inalámbricas modernas. Aunque se han realizado mejoras significativas con la introducción de Wi-Fi Protected Access (WPA) y posteriormente WPA2 y WPA3, aún enfrentan desafíos y debilidades. La adopción generalizada de WPA2 ha sido un paso positivo hacia una mayor seguridad, pero aún se observan vulnerabilidades, como el riesgo de ataque de diccionario debido a contraseñas débiles. La última versión, WPA3, ha introducido mejoras en la autenticación, lo que ofrece una mayor protección contra ataques de fuerza bruta, pero su implementación aún es relativamente limitada en la industria.

En relación con el Internet de las Cosas (IoT), se identificó que la proliferación de dispositivos conectados ha introducido nuevos desafíos de seguridad en las redes inalámbricas. Muchos dispositivos IoT carecen de medidas de seguridad adecuadas, lo que crea puntos débiles en la red. Los ataques dirigidos a estos dispositivos pueden comprometer la privacidad de los usuarios y facilitar el acceso no autorizado a la red. La segmentación de redes y la aplicación de políticas de seguridad específicas para los dispositivos IoT se han destacado como estrategias fundamentales para mitigar estos riesgos.

Con respecto a la tecnología 5G, se observó que, si bien ha brindado beneficios significativos en términos de velocidad y capacidad de las redes inalámbricas, también ha planteado nuevos desafíos de seguridad. La virtualización y compartición de recursos

en arquitecturas 5G pueden aumentar las superficies de ataque y, por lo tanto, es necesario abordar adecuadamente los desafíos de autenticación y privacidad asociados.

El impacto en la seguridad de las redes inalámbricas en un mundo cada vez más conectado y dependiente de la tecnología inalámbrica. A través de una revisión exhaustiva de la literatura y el análisis de los protocolos de seguridad, las amenazas emergentes y las implicaciones de la tecnología 5G, hemos identificado áreas clave de preocupación y oportunidades para mejorar la protección de estas redes vitales.

En cuanto a los protocolos de seguridad, se ha observado que, si bien ha habido mejoras significativas en la evolución de los protocolos, aún enfrentan desafíos y debilidades que requieren una atención continua. Protocolos más antiguos, como WEP, se han demostrado altamente vulnerables y, por lo tanto, su uso se desaconseja en entornos modernos. Los protocolos más recientes, como WPA2 y WPA3, ofrecen mejoras significativas en la autenticación y el cifrado, pero también enfrentan desafíos de seguridad, como el ataque de diccionario. En este sentido, es esencial fomentar la investigación y el desarrollo de protocolos de seguridad más robustos y resistentes a los ataques para garantizar una protección efectiva de las redes inalámbricas.

Además, se ha identificado que la proliferación del Internet de las Cosas (IoT) ha añadido nuevas complejidades a la seguridad de las redes inalámbricas. La falta de medidas de seguridad adecuadas en muchos dispositivos IoT representa una preocupación significativa y crea puntos débiles potenciales en la red. La segmentación de redes y la implementación de políticas de seguridad específicas para los dispositivos IoT son esenciales para mitigar los riesgos asociados con este panorama en constante crecimiento.

La adopción generalizada de la tecnología 5G ha brindado mejoras en la velocidad y capacidad de las redes inalámbricas. Sin embargo, esta revolución también ha planteado nuevos desafíos de seguridad, como la virtualización y compartición de recursos, que podrían abrir nuevas superficies de ataque. Para garantizar que la 5G cumpla con sus promesas de conectividad y eficiencia, es fundamental implementar soluciones de seguridad adaptadas y abordar adecuadamente los desafíos de autenticación y privacidad asociados con esta tecnología emergente.

Por último, se ha reconocido el potencial de la inteligencia artificial (IA) en la detección y prevención de amenazas en redes inalámbricas. El uso de IA y aprendizaje automático para analizar patrones de tráfico y detectar comportamientos anómalos ofrece una ventaja significativa en la lucha contra los ataques cibernéticos. La continua investigación y adopción de soluciones de IA en la seguridad de redes inalámbricas mejorarán la resiliencia de estas redes frente a las amenazas en constante evolución.

Conclusiones

En conclusión, la seguridad de las redes inalámbricas sigue siendo un desafío constante debido a la evolución tecnológica y el aumento de las amenazas cibernéticas. Sin embargo, los avances en protocolos de seguridad y el uso de tecnologías emergentes como la IA están teniendo un impacto significativo en la mitigación de riesgos y la protección de la información en entornos inalámbricos. A medida que la tecnología continúa evolucionando, es imperativo que los responsables de la seguridad se mantengan actualizados y adopten enfoques proactivos para garantizar la integridad y confidencialidad de las redes inalámbricas en el futuro.

El impacto en la seguridad de las redes inalámbricas es un tema crítico en la era digital actual. Las evoluciones en las amenazas, los protocolos de seguridad, el auge del IoT,

la adopción de la 5G y el papel de la IA en la detección de amenazas, todos contribuyen a un escenario complejo y cambiante. Abordar estos desafíos con enfoques proactivos y soluciones innovadoras es esencial para proteger la integridad y la privacidad de las redes inalámbricas y garantizar la confianza en su uso en entornos críticos y cotidianos. Como comunidad científica, es nuestro deber continuar investigando, colaborando y compartiendo conocimientos para fortalecer la seguridad de las redes inalámbricas y mitigar las amenazas en constante evolución.

Para mejorar la seguridad de las redes inalámbricas se recomienda abordar la adopción de mejores prácticas en la configuración de redes, la actualización de protocolos de seguridad, el fortalecimiento de la autenticación o la incorporación de tecnologías emergentes como la inteligencia artificial para mejorar la detección y mitigación de amenazas.

Bibliografía

ciberriesgos.com. ciberriesgos.com. 2023. https://www.ciberriesgos.com/por-que-el-protocolo-wep-no-es-seguro/ (último acceso: 12 de septiembre de 2023).

danielbenvenuto.com. 2023. https://danielbenvenuto.com/EDUCACION/LRA/Unidad%20I/Seguridad-WIFI.htm (último acceso: 12 de septiembre de 2023).

EcuRed. 2023. https://www.ecured.cu/Seguridad_en_redes_inal%C3%A1mbricas (último acceso: 12 de septiembre de 2023).

Ocampo, M. J. Ingeniería en Informática. Universidad Gran Asunción, 2018.

Ramírez, M, C Polanco, y B Farías. Seguridad Inalámbrica. Universidad Técnica Federico Santa María, s.f.

Cómo citar: Borrero Neninger, J. C., & Ponce Guerrero , J. L. (2023). Impacto en la seguridad de las redes inalámbricas. Journal TechInnovation, 2(1), 62–71. Recuperado a partir de https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/43