José Eduardo Gutiérrez Conejo - 2019073558

Redes

Lectura 7: Common Security Protocols for Wireless Networks

- WEP (Wired Equivalent Privacy) fue uno de los primeros protocolos de seguridad para redes inalámbricas, diseñado con la intención de ofrecer un nivel de privacidad comparable al de una red cableada. Utilizaba el algoritmo de cifrado RC4, sin embargo, se descubrieron debilidades rápidamente, como resultado, WEP se considera obsoleto e inseguro en la actualidad.

- WPA (Wi-Fi Protected Access) surgió como una solución interina ante las fallas de WEP. Introdujo mejoras como el uso del protocolo TKIP (Temporal Key Integrity Protocol), que ofrecía una gestión dinámica de claves.También incluyó autenticación mediante 802.1X y soporte para servidores RADIUS, lo que permitía un control más robusto del acceso. Aunque WPA mejoró considerablemente la seguridad, TKIP todavía presentaba vulnerabilidades y se basaba en parte en el mismo algoritmo RC4, lo que limitaba su eficacia a largo plazo.

- WPA2, por su parte, fue más segura y robusta al adoptar el protocolo de cifrado AES (Advanced Encryption Standard) junto con CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), eliminando el uso de RC4 y superando las limitaciones de TKIP. WPA2 ofrece un nivel de seguridad mucho más alto y se convirtió en el estándar obligatorio para dispositivos certificados por la Wi-Fi Alliance a partir de 2006.