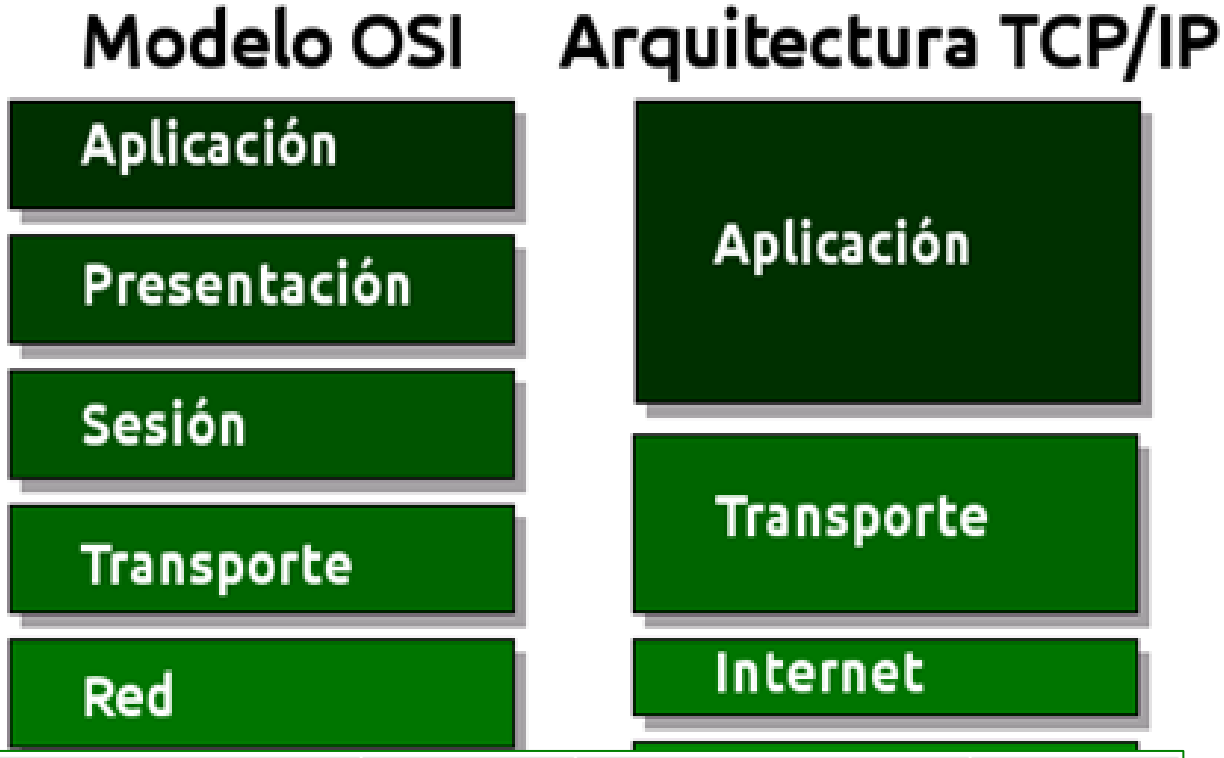
Unidades V y VI: Criptografía en Redes

Redes Wireless. Implementación WEP 64 bits y 128 bits. Manejo de Múltiples Claves. Implementación y riesgos de RC4. Scrambling. Implementación de WPA. Análisis de AES sobre Wifi. MAC

El modelo OSI y las redes WiFi



Generación/Estándar del IEEE	la frecuencia	Velocidad de enlace máxima	Año
Wi-Fi 6 (802.11ax)	2,4/5 GHz	600–9608 Mbit/s	2019
Wi-Fi 5 (802.11ac)	5 GHz	433–6933 Mbit/s	2014
Wi-Fi 4 (802.11n)	2,4/5 GHz	72–600 Mbit/s	2009

Seguridad en redes WiFi

Generación/Estándar del IEEE
Wi-Fi 6 (802.11ax)
Wi-Fi 5 (802.11ac)
Wi-Fi 4 (802.11n)

- **WEP** (Wired Equivalent Privacy), es la norma de seguridad 802.11.
- **WPA** (Wi-Fi Protected Access), es la norma 802.11i.
- **WPA2/802.11i** (Wi-Fi de Protected Access2).
- **WPA3/ 802.11ac >> 802.11ax** (Wi-Fi de Protected Access3).

Seguridad WEP vs. WPA/WPA2

Tabla 1. Evolución de sistemas de codificación inalámbrica

Sistema de encriptación	WEP	WPA	WPA2
Estándar	802.11b	802.11g	802.11i
Algoritmo	RC4	RC4TKIP	AES (Rijndael)
Características	Protección a redes inalámbricas vulnerables	IV extendido Llaves dinámicas (TKIP) Incluye MAC del emisor	Número algoritmo de mayor complejidad Tramas convertidas por operaciones matriciales
Longitud de claves	**64 (40) o 128 (104) bits**	**128 a 256 bits**	**128 a 256 bits**
Vulnerabilidad	IV muy corto Llaves estáticas Claves cortas Chequeo de integridad independiente de datos cifrados	Autenticación por handshake auditable. Claves en diccionario, o reconocibles por atacante	Claves conocidas Rondas cortas en información muy confidencial Uso de claves en diccionario o conocidas por atacante
Ataques conocidos	FMS, por estadística de IV, muy exitoso, obteniendo gran cantidad de tramas con IV	Por fuerza bruta comparando claves con handshake, éxito dependiente de tener la clave en el diccionario	Por fuerza bruta muy lenta comparando directamente con la red claves de diccionario, muy poco éxito en bastante tiempo de ataque

Fuente: elaboración propia

- Counter Mode CBC-MAC Protocol (**AES CCMP**) reemplazó a **TKIP**
- **WPA2-CCMP** (**WPA2-PSK-CCMP**) y puede ser utilizado con (**WPA-CCMP / WPA-PSK-CCMP**).

https://ntrrgc.me/attachments/Cifrado_RC4/
http://www.scielo.org.co/pdf/tecn/v19nspe/v19nspea07.pdf
https://www.acrylicwifi.com/blog/que-es-wpa-psk-tkip-ccmp/

Seguridad en WPA3

El WPA3 incluye las siguientes actualizaciones:

- Cambios en el protocolo de autenticación / asociación para utilizar la autenticación simultánea de iguales (SAE).
  - El uso de SAE es una respuesta directa a una debilidad identificada en el protocolo de enlace de 4 vías WPA2 descubierto por Vanhoef en 2017 (conocido como KRACK). https://www.kaspersky.es/resource-center/definitions/krack
  - Aunque hay actualizaciones disponibles para protegerse del "ataque KRACK", el uso de SAE mejora el proceso de administración de claves utilizado para el cifrado del enlace y proporciona otros beneficios.
  - Dado que las claves utilizadas para el cifrado se basan en sesiones, no están vinculadas a un PSK estático, un intruso ya no podrá capturar cantidades de tráfico inalámbrico y trabajar fuera de línea para determinar la contraseña compartida.
  - Del mismo modo, cualquier ataque de fuerza bruta se limitará a una sola sesión. Como resultado, cualquier dato histórico está protegido en caso de que se vulnere una clave para una sesión específica.

Debilidad WPA2 resuelta por WPA3

KRACK: debilidad identificada en el protocolo de enlace de 4 vías WPA2 descubierto por Vanhoef en 2017

El **KRACK afecta al tercer paso** del handshake:

- Permite que el atacante manipule y reproduzca la clave de cifrado WPA2 para engañarlo e instalar una clave que ya está en uso.
- Una vez que se ha reinstalado la clave, se restablecen a sus valores originales otros parámetros asociados con ella, que son el número de paquetes transmitidos progresivamente, llamado "nonce", y el contador de reproducción.
- En lugar de cambiar al cuarto paso del handshake, el nonce se restablece continuamente para reproducir transmisiones del tercer paso.
- Así se establece el protocolo de cifrado para el ataque y, en función de cómo los atacantes reproduzcan las transmisiones del tercer paso, pueden vulnerar la seguridad Wi-Fi.

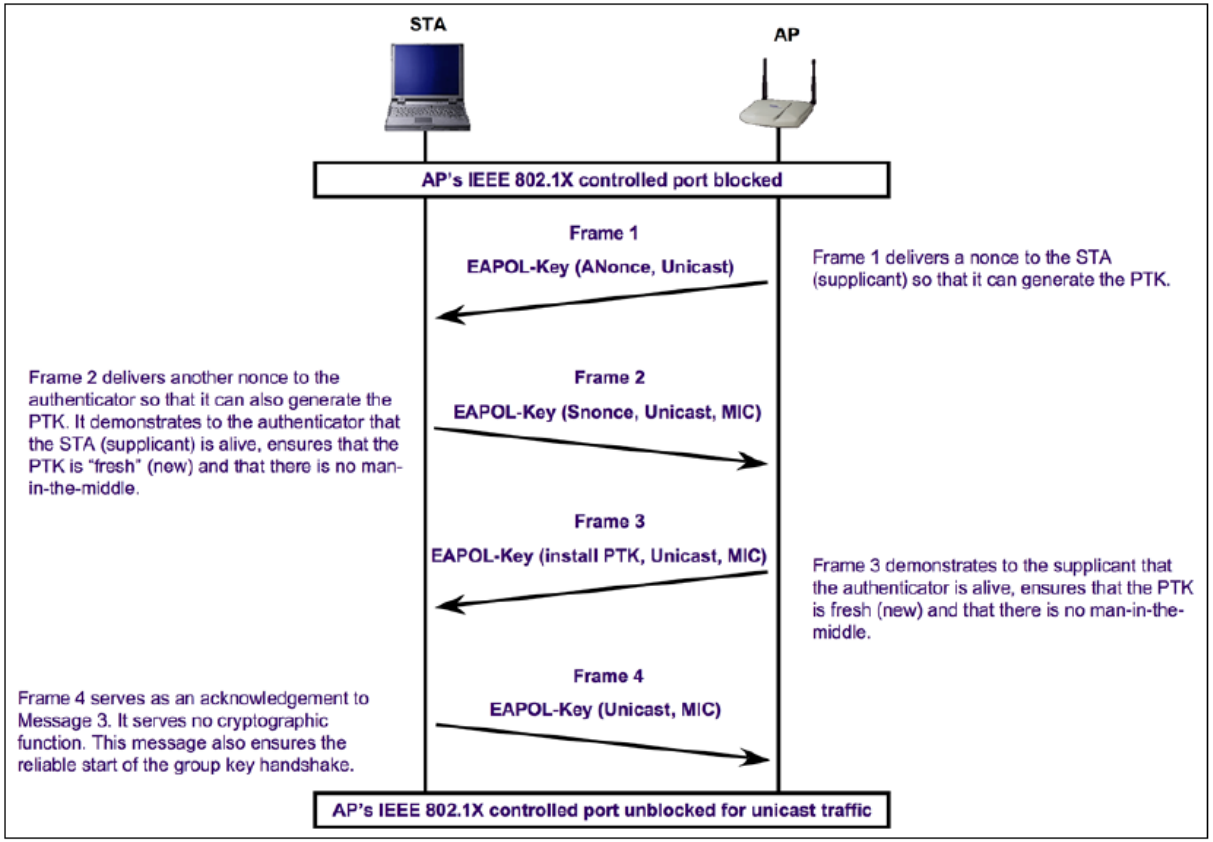


Figure 5-14. 4-Way Handshake

Seguridad en WPA3

El WPA3 incluye las siguientes actualizaciones:

- Aumento del tamaño de la clave de enlace cuando se usa la autenticación Enterprise (EAP) a 192 bits.
- Adición de cifrado inalámbrico oportunista (OWE) llamado Wi-Fi CERTIFIED Enhanced Open. https://datatracker.ietf.org/doc/html/rfc8110
- Adición de la incorporación simplificada de dispositivos sin cabeza mediante el protocolo de aprovisionamiento de dispositivos llamado Wi-Fi CERTIFIED Easy Connect.
- Primitivas del modo WPA3-Enterprise 192-bit:
  - Intercambio de claves: Curva elíptica Diffie-Hellman Efímera (ECDHE)
  - Autenticación: Algoritmo de firma digital de curva elíptica (ECDSA)
  - Cifrado: AEAD Estándar de cifrado avanzado con clave de 256 bits en modo Galois / Contador (AES 256 GCM)
  - Integridad: Algoritmo hash seguro 384 (SHA384)

https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v2.0.pdf