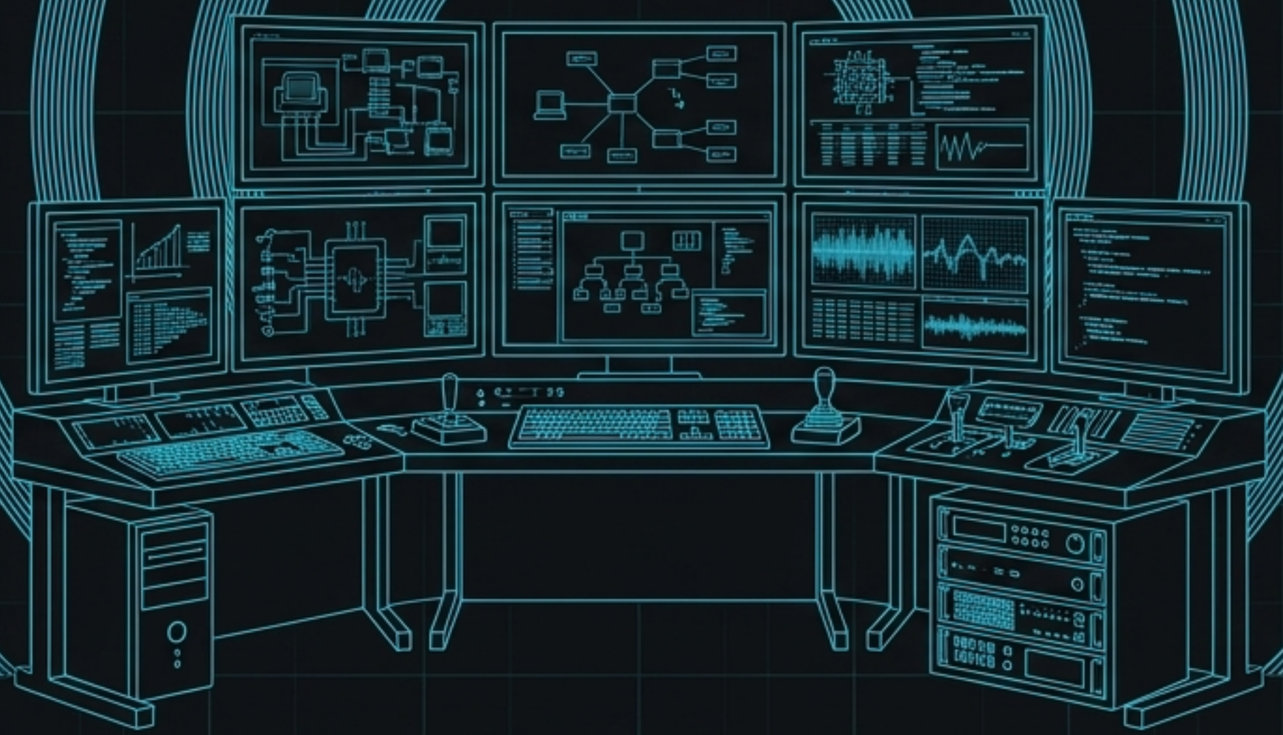
Serie IoT Red Teaming | Nivel: Intermedio/Avanzado.

El Manual Táctico de Hacking Inalámbrico

Diseccionando vulnerabilidades en Wi-Fi, Bluetooth y Radiofrecuencia (RF).



La ilusión de la seguridad física

Las redes transmiten datos en todas direcciones. Cualquiera en el rango puede escuchar.

Los periféricos de corto alcance a menudo omiten cifrados fuertes por conveniencia.

OPEN

Los sistemas físicos (cerraduras, alarmas) confían ciegamente en señales invisibles.

El atacante no necesita romper la puerta; solo necesita capturar la frecuencia correcta.

EVALUACIÓN: VULNERABILIDAD CRÍTICA DETECTADA.
PROTOCOLOS DE CIFRADO REQUERIDOS.

Parámetros Legales y Éticos (Regla de Oro: No Causar Daño)

Autorizado

- Pruebas en redes propias (Laboratorio aislado)
- Contratos de Penetration Testing firmados
- Participación en Bug Bounties y CTFs
- Divulgación responsable (Responsible Disclosure)

Delito

- Acceso sin autorización explícita
- Intercepción pasiva en Wi-Fi público (Wiretap Act)
- Crackeo de contraseñas de terceros
- Despliegue de Evil Twins maliciosos

La ignorancia no es defensa legal. La Ley de Abuso y Fraude Informático (CFAA) penaliza el acceso no autorizado como delito federal.

El Centro de Comando: Hardware y Software

Capa Wi-Fi

Hardware

Alfa AWUS036ACH
Panda PAU09 (Modo Monitor)

Software

Aircrack-ng (Crackeo)
Wireshark (Análisis)
Kismet (Descubrimiento pasivo)

Capa Bluetooth

Hardware

Ubertooth One

Software

BlueZ (Stack Linux)
Btlejack (Sniffing BLE)

Capa RF & RFID

RTL-SDR
HackRF One
Yard Stick One
Proxmark3
Flipper Zero

Software

GQRX
RTL_433
GNURadio

La Matriz del Espectro Inalámbrico

Diagnostico diagnóstico	Wi-Fi (802.11)	Bluetooth (BR/EDR/BLE)	Radiofrecuencia (Sub-GHz/RFID)
Uso Principal	Internet / Redes Locales	Periféricos / Audio / IoT	Control de Acceso / Domótica
Alcance Operativo	Largo (10m - 100m+)	Corto (1m - 10m)	Variable (Milímetros a Kilómetros)
Vector Crítico de Ataque	Intercepción de Handshakes y APs Falsos	Emparejamiento Débil (Bluebugging)	Replay Attacks y Clonación de Señales

TACTICAL CYBER-BLUEPRINT

La Evolución del Estándar 802.11

802.11b/a (11-54 Mbps).
Nacimiento del Wi-Fi. Altamente vulnerable (WEP).

802.11g (54 Mbps).
Estándar dominante. Transición a WPA.

802.11n (Wi-Fi 4) (600 Mbps).
Introducción de MIMO. Doble banda (2.4/5GHz).

802.11ac (Wi-Fi 5) (3.5 Gbps).
MU-MIMO exclusivo en 5GHz.

802.11ax (Wi-Fi 6) (9.6 Gbps).
OFDMA y WPA3 integrados. Optimizado para entornos IoT densos.

1999

2003

2009
2.4GHz 5GHz

2014
2.4GHz 5GHz

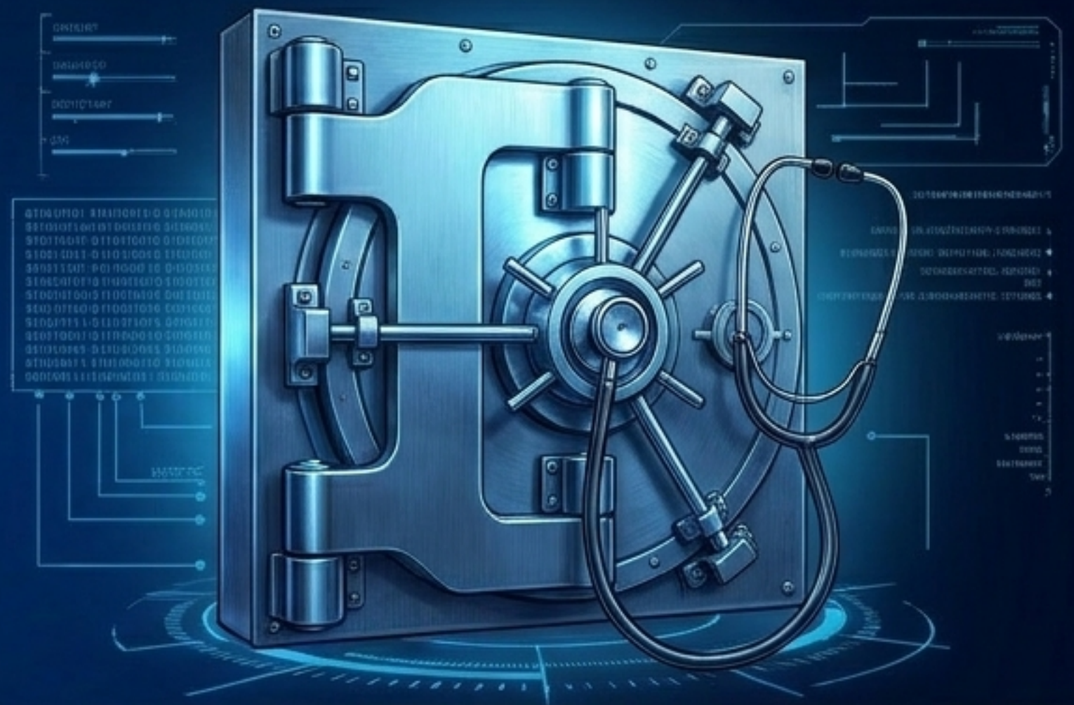
2019+
2.4GHz 5GHz

Anatomía del Cifrado: De WEP a WPA3

WEP	WPA	WPA2	WPA3
Tecnología: RC4 (Claves de 40/104 bits)	**Tecnología:** TKIP (Claves dinámicas)	**Tecnología:** AES-CCMP (Cifrado militar)	**Tecnología:** GCMP-256 / SAE
Falla Crítica: Reutilización de Vectores de Inicialización (IVs cortos)	**Falla Crítica:** Vulnerable a ataques de fuerza bruta sobre claves precompartidas (PSK)	**Falla Crítica:** Ataque KRACK (2017) en el 4-way handshake	**Ventaja:** SAE mitiga ataques de fuerza bruta offline y provee Forward Secrecy
Tiempo de Ruptura: < 60 segundos con Aircrack-ng			**Riesgo:** Ataques de degradación a WPA2

TACTICAL CYBER BLUEPRINT

¿Por qué fallan los cifrados?



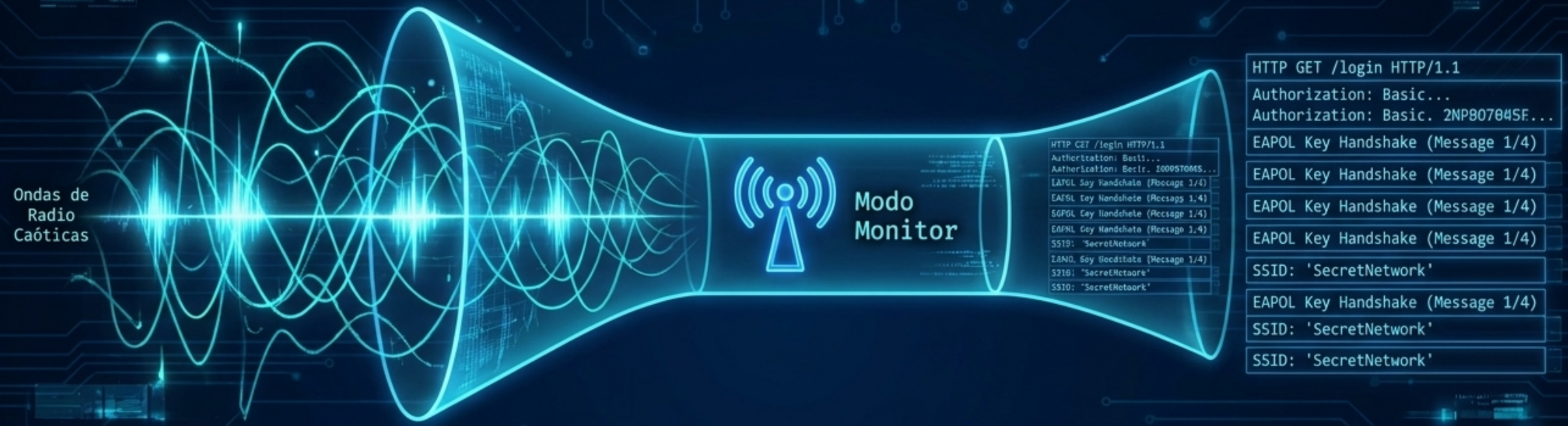
El Candado Roto (WEP)

Los Vectores de Inicialización (IVs) son como dejar la llave pegada al candado. El atacante solo necesita recolectar suficientes paquetes para encontrar la clave repetida.

La Bóveda Escuchada (WPA2)

WPA2 es un candado fuerte, pero el proceso de apertura (el 4-way handshake) es ruidoso. Un atacante captura la “conversación” de autenticación, se la lleva a casa, y prueba millones de claves en la sombra usando diccionarios offline.

El Embudo de Intercepción: Wireshark y Tcpdump



1 Paso 1: Modo Monitor

`airmon-ng start wlan0.`

Tarjeta Wi-Fi configurada para leer todo el tráfico aéreo, no solo el dirigido a ella.

2 Paso 2: Captura (Tcpdump)

Herramienta CLI para grabar datos crudos. Ejemplo: `tcpdump -i wlan0 ether proto 0x888e` (captura exclusiva de handshakes WPA2).

3 Paso 3: Análisis (Wireshark)

Interfaz gráfica para filtrar la aguja en el pajar. Ejemplo: `wlan.fc.type_subtype == 0x0c` (detecta paquetes de desautenticación). Si la red es abierta (HTTP), las contraseñas viajan en texto plano.

TACTICAL CYBER BLUEPRINT

Arquitectura del Gemelo Malvado (Evil Twin)

1 **El Cebo**: El atacante clona el nombre de red (SSID) legítimo usando herramientas como herramientas como Wi-Fi Pineapple.

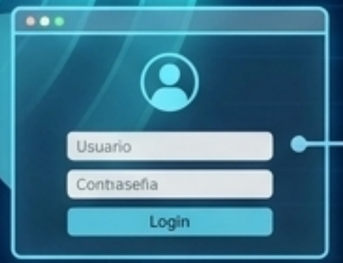
2 **El Secuestro (Karma Attack):** Transmitiendo con mayor potencia, obliga a los dispositivos a auto-conectarse a la red falsa.

Real AP
(Coffee_WiFi)

Internet Real

Víctima

Atacante
(Evil Twin)

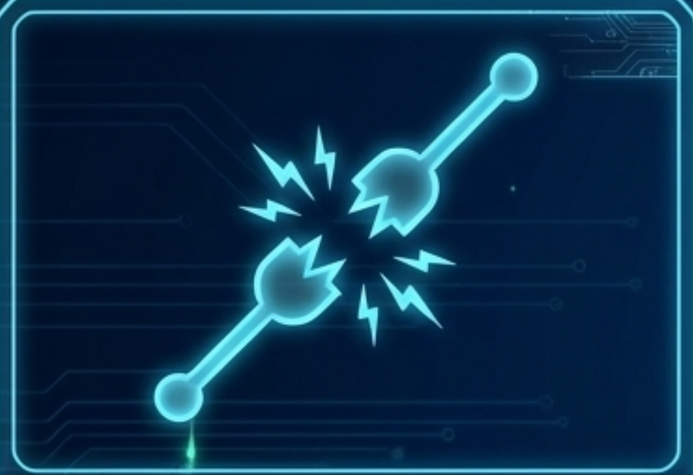


Captive Portal

3 **El Portal Cautivo:** La víctima es redirigida a una página de inicio de sesión falsa, entregando credenciales directamente al atacante (MITM).

TACTICAL CYBER BLUEPRINT

Glosario de Ataques Wi-Fi (Capa 802.11)



Ataque de Desautenticación (Deauth)

Falsificación de tramas de gestión (management frames) no cifradas. Desconecta usuarios legítimos a la fuerza para forzar reconexiones y capturar handshakes.

`Herramienta: mdk3, aireplay-ng`

PMKID Attack

Extrae el PMKID directamente del router sin necesidad de que un cliente esté conectado. Permite crackear WPA/WPA2 más rápido sin esperar un handshake completo.

Explotación WPS

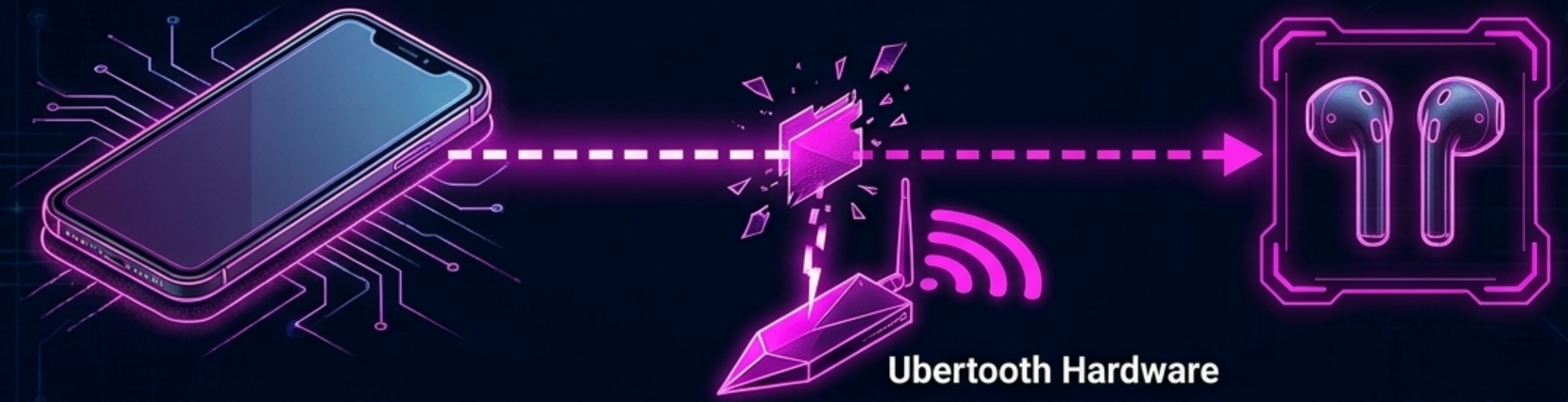
Ataque de fuerza bruta contra los pines débiles de configuración rápida del router.

`Herramienta: Reaver`

Mitigación inmediata:
Desactivar WPS en el router.

Vectores de Ataque Bluetooth (BR/EDR y BLE)

Vulnerabilidad Estructural:
Muchos dispositivos confían en pines por defecto (0000, 1234) o emparejamientos débiles (Just Works).



Bluejacking

Envío de mensajes o contactos no solicitados a dispositivos vulnerables. Principalmente una molestia técnica.

Bluesnarfing

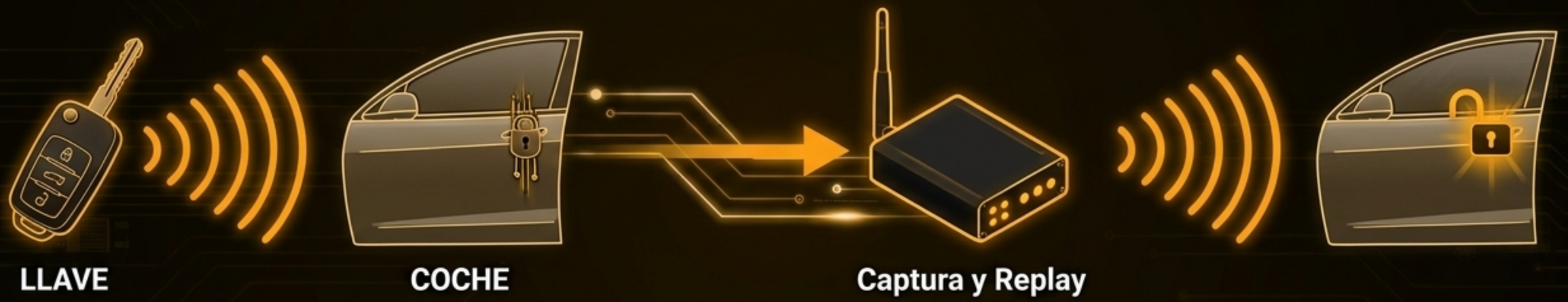
Robo silencioso de contactos, mensajes y archivos al explotar fallas de autenticación.

BlueBorne & Bluebugging

Ejecución remota de código (RCE) que otorga control total del dispositivo sin necesidad de emparejamiento.

Explotación de Radiofrecuencia (SDR e IoT)

El Problema del Texto Plano en RF:
Domótica (Zigbee/Z-Wave), llaves de autos, y controles industriales a menudo transmiten comandos analógicos sin cifrar.



Ataque RollJam

Interfiere la señal de código rodante (rolling code) del usuario, captura el código válido y transmite un código antiguo para engañar al sistema.

Signal Jamming

Inundar la frecuencia con ruido para desconectar cámaras de seguridad o alarmas inalámbricas.

El Ecosistema de Amenazas Omnidireccional

Síntesis Operativa:
En el mundo real, los ataques no ocurren de forma aislada. Una superficie de ataque moderna expone expone simultáneamente múltiples protocolos.

El Ataque Combinado:
El atacante bloquea la cámara RF (Jamming), desautentica el termostato de la red Wi-Fi (Deauth) y captura la reconexión reconexión WPA2 (Handshake Sniffing)—todo sin bajarse del auto.

Conclusión: La seguridad de la red es tan fuerte como su protocolo inalámbrico más débil.

Estrategia Defensiva Unificada (Bloqueando el Perímetro)

Blindaje Wi-Fi

✓ Migrar a WPA3. ✓ Desactivar WPS de forma permanente. ✓ Usar VPN en redes públicas. ✓ Implementar Segmentación de Red (aislar IoT en una VLAN separada). ✓ Habilitar PMF (Protected Management Frames) contra deauth.

Blindaje Bluetooth

✓ Apagar BT cuando no esté en uso. ✓ Usar modo Oculto/No Descubrible. ✓ Eliminar emparejamientos antiguos.

Blindaje RF/IoT

✓ Cambiar credenciales de fábrica. ✓ Exigir dispositivos con códigos rodantes (Rolling Codes) y cifrado AES-128. Actualizar firmware regularmente.

Mantén la paranoia. Mantente actualizado.
Si es inalámbrico, asume que alguien está escuchando.