



INFORME TÉCNICO FORENSE: VULNERABILIDAD KEYLESS (RELAY ATTACK) Y APANTALLAMIENTO RF

Despiece electromagnético de sistemas PKE (125 kHz / 433-868 MHz), cronometría del vector de ataque y física de apantallamiento Faraday.

OBJETO Y ALCANCE DEL ESTUDIO

Análisis de la vulnerabilidad estructural en sistemas de entrada y arranque sin llave (Passive Keyless Entry & Start, PKE). En 2026, más del 85% de los robos de vehículos sin rotura física se ejecutan mediante amplificación de señal (Relay Attack) burlando la autenticación criptográfica legítima sin alterar la llave del usuario.

1. ARQUITECTURA DE RADIOFRECUENCIA DE LOS SISTEMAS KEYLESS

Los sistemas PKE estándar operan mediante un canal de radiofrecuencia dual asimétrico concebido bajo la asunción de proximidad física:

- Canal de Interrogación LF (125 kHz / 134.2 kHz): Las antenas en las manetas del coche emiten un campo magnético inductivo de corto alcance (<1.5 m) que excita la bobina 3D de la llave.
- Canal de Respuesta UHF (433.92 MHz en Europa / 315 MHz en EE.UU. / 868 MHz): El microcontrolador de la llave procesa el desafío criptográfico y emite el token cifrado a la ECU.
- Vector de Vulnerabilidad: El protocolo clásico valida la firma criptográfica (AES-128 / Hitag), pero NO mide el tiempo de propagación (Time-of-Flight), permitiendo amplificar la señal a más de 300 metros.

2. CRONOMETRÍA Y SECUENCIA FORENSE DEL ATAQUE RELAY (< 25 SEGUNDOS)

Fase / Tiempo	Ubicación Atacante	Acción Electromagnética	Respuesta del Sistema
Fase 1 (T=0.0s)	Atacante 1 (Junto al Coche)	Toca la maneta capacitiva del vehículo	ECU emite ráfaga LF 125 kHz
Fase 2 (T=0.3s)	Atacante 1 -> Atacante 2	Antena capta LF y modula en 2.4 GHz	Puente RF de alta potencia hacia la vivienda
Fase 3 (T=0.6s)	Atacante 2 (Fachada/Puerta)	Emisor reproduce la señal LF de 125 kHz	Llave en el receptor despierta y firma
Fase 4 (T=0.9s)	Atacante 2 -> Atacante 1	Captura respuesta UHF 433 MHz y retransmite	Coche valida firma: abre puertas y arranca

ESQUEMA FORENSE DE PROPAGACIÓN ELECTROMAGNÉTICA:





3. FÍSICA DEL APANTALLAMIENTO: EFECTO PELICULAR Y JAULAS DE FARADAY

El principio de la Jaula de Faraday establece que las cargas eléctricas de un conductor hueco cerrado se distribuyen en su superficie exterior, cancelando el campo eléctrico en el interior. Para bloquear campos electromagnéticos en el rango de 100 kHz a 6 GHz, se evalúa la atenuación en decibelios (dB):

Material de Blindaje	Atenuación dB	Rango Frecuencias	Durabilidad / Riesgos	Eficacia Antirrobo
Aluminio Macizo CNC 6061	> 95 dB	10 kHz - 10 GHz	Inmune al desgaste / Hermético	100% Blindaje Militar (Óptimo)
Cobre-Níquel Ripstop (Doble Capa)	> 85 dB	100 kHz - 30 GHz	Excelente / Requiere cierre solapado	99.8% Eficacia (Recomendado)
Fundas Plegables Monocapa Baratas	< 40 dB	Banda estrecha	Microfisuras por flexión en 30 días	Insuficiente (Fugas RF detectadas)
Lata metálica de cocina casera	< 25 dB	Discontinua	Falta de sellado RF en la tapa	Insegura (Apertura por resonancia)

4. PROTOCOLO DE VERIFICACIÓN PRÁCTICA EN 4 PASOS (TEST DE CAMPO)

- ☐ **Paso 1: Test de Contacto Directo en Tirador**
Introduce la llave dentro de la caja o funda Faraday cerrada. Acércate a menos de 5 cm de la manilla del coche e intenta abrir. El coche DEBE permanecer totalmente bloqueado.
- ☐ **Paso 2: Test de Arranque Interior**
Entra al vehículo (abriendo previamente), cierra la caja Faraday con la llave dentro y presiona el botón Start. El cuadro debe indicar "Llave no detectada".
- ☐ **Paso 3: Blindaje de la Segunda Llave (Copia de Respaldo)**
Guarda permanentemente la llave de repuesto dentro de una caja Faraday en el hogar. El 40% de los robos aprovechan llaves secundarias sin proteger.
- ☐ **Paso 4: Distancia de Seguridad en el Hogar**
Ubica la caja Faraday a más de 5 metros de puertas exteriores o ventanas para degradar la ganancia de antenas direccionales.

5. EVOLUCIÓN TECNOLÓGICA: ULTRA-WIDEBAND (UWB IEEE 802.15.4z)

Los vehículos modernos (BMW Digital Key Plus, Audi) están migrando a Ultra-Wideband (UWB). UWB mide el Tiempo de Vuelo (Time-of-Flight, ToF) de pulsos de nanosegundos a la velocidad de la luz. Como un repetidor de radio añade latencia inevitable por conmutación (>50 ns), el coche detecta que la señal proviene de lejos y rechaza el acceso automáticamente.

6. MARCO NORMATIVO Y BIBLIOGRAFÍA CIENTÍFICA

- * ETSI EN 300 220-1: Short Range Devices (SRD) operating in the frequency range 25 MHz to 1000 MHz — ETSI
- * ADAC Keyless Report 2025/2026: Security Vulnerability Index on 500+ Tested Keyless Vehicles — ADAC Alemania
- * IEEE 802.15.4z-2020: Enhanced Ultra-Wideband (UWB) Physical Layer and Ranging Extension — IEEE Standards
- * NIST SP 800-98: Guidelines for Securing Radio Frequency Identification (RFID) Systems — NIST

RECURSOS Y ASISTENCIA TÉCNICA:

[Consultar Asesor IA en Telegram](#)

[Ver análisis completo en CandadoInteligente.com](#)