CERIAS

The Center for Education and Research in Information Assurance and Security

SpectralDNA

Stephen Glombicki, Jacob Jannotta
sglombic@purdue.edu, jjannott@purdue.edu

Motivation

Today's world is saturated with invisible signals. Every device we carry and every system we use emits patterns across the radio frequency spectrum. This research examines the distinct electromagnetic signatures that individuals and their technologies continuously broadcast, forming digital fingerprints that can be measured, analyzed, and potentially identified.

Abstract

SpectralDNA investigates whether an individual can be reliably **distinguished** using only the ambient radio frequency emissions produced by the devices they carry and use. We perform **passive**, **non intrusive** captures with software defined radio and extract **observable** features. These features include protocol fields exposed in **broadcast** or **discovery** traffic as well as signal and **timing** characteristics that persist across **short** capture windows. We then **fuse** the heterogeneous observations into a single composite profile per subject and evaluate how consistently that profile can be re linked across sessions and environments, even when some protocols employ rotation or randomization.

Our findings reveal that the combination of signals emitted by a single person's ecosystem of devices constitutes a multi-layered identifier effectively forming a unique "**Spectral DNA**".

Methodologies

Using a **HackRF One software-defined radio**, we performed passive captures across nine distinct frequency bands ranging from 315 MHz to 6 GHz. Each capture was processed to extract identifiable data points such as MAC addresses, device IDs, advertising payloads, and rolling codes. By cataloging these emissions across bands, we constructed **composite RF profiles** to evaluate how effectively individuals can be fingerprinted through their everyday device activity.

Results

Our research reveals a spectrum of anonymization across RF bands. Wi-Fi and BLE show the strongest privacy mitigations through MAC address randomization and rotating advertisements. Cellular protocols offer limited protections via temporary identifiers, but **frequency-band analysis** still enables reliable fingerprinting. Most concerning, ANT/ANT+, GPS/GNSS, TPMS, and key fob/RKE signals have no meaningful anonymization, broadcasting static, identifiable data in the clear. The combination of these signals generally creates a **multi-layered fingerprint** that is **highly unique** to each individual regardless of occasional protections, allowing for **easy identification** and **persistent tracking** within a short period of time.

BAND	COLLECTING	EXAMPLE CAPTURE
Wi-Fi 2.4 / 5 GHz 802.11a/b/g/n/ac	• SSID Broadcasts • MAC Address • Carrier Freq Offset	ssid "PAL3.0" · "eduroam" · mac A4:83:E7:2F:B1:04 · cfo **-1.247 kHz**
FP: 1 in 8 — MAC randomization, common SSIDs		
Bluetooth LE 2402 MHz Ch 37 / 38 / 39	• Adv Payload • Manufacturer Data • Adv Interval / Jitter	mfr 0×004C (Apple Inc.) · interval **48.2 ms ± 0.3 ms** · drift **+3.2 ppm**
FP: 1 in 128 — addr randomization, Apple saturation		
Cellular LTE 700 MHz B2 · B4 · B12 · B41 · B71	• IMSI / IMEI • IQ Imbalance • PA Nonlinearities	imei 35391210XXXXXXX · iq **0.42 dB · 2.1° phase** · cell eNB 148276 · PCI 214
FP: 1 in 1,200 — IMEI strong, passive capture difficult		
5G NR sub-6 3.7 GHz n41 · n77 · n78 C-band	• Beam Pattern • SSB Burst Timing • Clock Drift	nrci 4829103872 · drift **+2.14 kHz** · beam SSB idx 4 · -89 dBm
FP: 1 in 250 — fewer distinguishing features		
ANT / ANT+ 2.4 GHz ISM · fitness devices	• Device Profile • Device Number • TX Characteristics	dev 0xB4E2 · Garmin FR 265 · profile HR Monitor · Type 120 · tx **0 dBm GFSK**
FP: 1 in 6 — limited protocol, few unique IDs		
GPS / GNSS 1575 MHz L1 · L2 · L5	• A-GPS / SUPL Requests • Location Leakage • Satellite Lock Pattern	supl supl.google.com:7275 · sats GLONASS 4/12 · loc **40.4237°N, 86.9212°W**
FP: 1 in 10 — location narrows, not unique alone		
TPMS 315 MHz OOK · unauthenticated	• Sensor IDs (×4) • Tire Pressure • Temperature	id[FL] 0xA4F82C01 · psi 32.1 / 32.4 / 31.8 / 32.0 · temp 72 / 71 / 73 / 72 °F
FP: 1 in 64,000 — 4 unique sensor IDs per vehicle		
Key Fobs / RKE 315 MHz ASK / OOK	• Rolling Code • Modulation Pattern • Power Ramp Profile	rolling 0×7E3BA91C · mod ASK · 3.2 kbps · ramp **4.8 µs**
FP: 1 in 128,000 — rolling codes highly unique		
ALL 8 COMBINED: <0.1% — virtually zero misidentification		

PURDUE UNIVERSITY

CERIAS