

RF Signals and Cybersecurity

Alan Lowne Saelig Co. Inc. CEO

An often-overlooked aspect of protecting systems, networks, devices, data, and programs from digital attacks, unauthorized access, theft, or damage is to ensure the **confidentiality, integrity, and availability** (known as the CIA triad) of information and digital services coming from unexpected sources: RF signals. Digital cybersecurity focuses on logical network layers, operating systems, and software, whereas Radio Frequency (RF) cybersecurity operates at the physical electromagnetic spectrum, securing wireless signals transmitted over the air.

The Core Pillars of Cybersecurity (The CIA Triad)

- **Confidentiality:** Ensuring that sensitive data is accessible only to authorized users (e.g., encryption, passwords, multi-factor authentication).
- **Integrity:** Safeguarding data from being altered, tampered with, or deleted by unauthorized entities (e.g., file hashing, access controls).
- **Availability:** Ensuring systems, networks, and data remain operational and accessible when authorized users need them (e.g., backup systems, DDoS mitigation).

Common Threats

- **Malware:** Malicious software designed to cause harm, including viruses, ransomware, trojans, and spyware.
- **Phishing:** Social engineering attacks where attackers impersonate trusted entities to trick individuals into revealing sensitive credentials or information.
- **Man-in-the-Middle (MitM) Attacks:** Intercepting communications between two parties to steal or alter data.
- **Denial-of-Service (DoS / DDoS):** Overwhelming a system or network with traffic to render it unavailable to legitimate users.

A Comparison Between Digital and RF Cybersecurity

Feature	Digital Cybersecurity	RF Cybersecurity
Domain & Environment	Logical, IP-based networks, software applications, cloud, and operating systems.	Physical electromagnetic (EM) spectrum, over-the-air signals, and hardware transceivers.
Technologies Involved	Firewalls, SIEM, VPNs, Endpoint Detection and Response (EDR), IAM.	Software Defined Radios (SDR), spectrum analyzers, direction finders, RF shielding.
Primary Vectors	Malware, phishing, SQL injection, unauthorized API access, logic flaws.	Signal jamming, signal spoofing, replay attacks, RF exfiltration, eavesdropping.
Defensive	Network segmentation, software patches,	Spectrum monitoring, frequency hopping, physical



Feature	Digital Cybersecurity	RF Cybersecurity
Mechanisms	digital encryption, access policies.	shielding (Faraday cages), directional antennas.
Core Skills	Programming, network routing (TCP/IP), system administration, cryptography.	Signal processing, physics, wave propagation, hardware design, modulation.

Key Differences

- **Attack Surface:** Digital cybersecurity protects structured data packets traversing cables, switches, and routers. RF cybersecurity defends unstructured, open-air transmissions that extend physically beyond secure perimeters, creating blind spots that standard firewalls cannot see.
- **Impact of Attacks:** A digital attack generally aims to exfiltrate data, corrupt software, or gain system privileges. An RF attack often disrupts physical connectivity directly—such as jamming GPS, spoofing drone signals, or intercepting IoT communications.
- **Defensive Boundary:** Digital security relies on logical access boundaries (passwords, firewalls, network ACLs). RF security requires managing physical space and frequency bands using signal intelligence and physical containment.

The two disciplines increasingly overlap in environments like Internet of Things (IoT), wireless sensor networks, aerospace, and critical infrastructure, where digital commands are delivered over radio waves.

RadGreen is a technology company that specializes in easy to deploy, next-generation RF monitoring solutions for corporate, commercial and government enterprises. Their RF monitors sense radiation levels in specific wavelength bands to provide online or audible alarms when preset thresholds are exceeded. Standalone, unconnected versions are available for connection-sensitive deployments.



Monitoring Radio Frequency (RF) levels has become a fundamental pillar of modern cybersecurity, particularly as organizations rely more heavily on wireless communication, Internet of Things (IoT) devices, and Operational Technology (OT). Traditional cybersecurity relies heavily on inspecting software, network packets, and IP-based firewalls. However, RF spectrum monitoring operates at **Layer 1 (the Physical Layer) of the OSI model**, capturing malicious activity that occurs before packets are processed by a network stack or logged by traditional security software.

RF monitoring is vital to a comprehensive cybersecurity strategy for several key reasons:

1. Eliminating Physical Layer "Blind Spots"

Traditional security monitoring tools like Firewalls, Intrusion Detection Systems (IDS), and Endpoint Detection and Response (EDR) agents operate at higher network layers (Layers 2–7).

- **Protocol Bypass:** Adversaries can exploit wireless protocols (Wi-Fi, Bluetooth, Zigbee, Cellular, proprietary RF) to establish covert communication channels that completely bypass network boundaries and firewalls.
- **Pre-Packet Detection:** Monitoring the RF spectrum allows security teams to detect unauthorized electromagnetic emissions or hardware intrusions before any data payload is delivered or processed by software.

2. Identifying Rogue Devices and "Air-Gap" Breaches

Air-gapping—physically isolating critical networks from the internet—is a standard security control for industrial control systems (ICS), defense networks, and critical infrastructure.

- **Unauthorized Transmitters:** Attackers can bypass air-gaps using rogue Wi-Fi access points, cellular modems, eavesdropping bugs, or unauthorized IoT devices plugged directly into internal infrastructure.
- **RF Fingerprinting:** Advanced RF monitoring tools establish baseline signal profiles and build unique RF fingerprints for authorized hardware. This enables real-time detection and precise localization of rogue transmitters or unauthorized devices operating within a facility.

3. Detecting Jamming, Interference, and Physical Attacks

Denial of Service (DoS) attacks at the RF level do not require hacking into software; they simply require transmitting noise or overpowering legitimate signals.

- **Signal Jamming:** Attackers can flood specific frequencies to disable critical communications—such as wireless alarms, automated guided vehicles (AGVs), remote SCADA sensors, or physical access control systems.
- **Operational Continuity:** Monitoring RF power levels and signal-to-noise ratios enables security operations to immediately distinguish between technical hardware failure, environmental noise, and intentional RF jamming.

4. Preventing Eavesdropping, Signal Replay, and Spoofing

Wireless signals naturally propagate beyond physical perimeters, allowing threat actors to intercept signals from parking lots or neighboring buildings.

- **Replay Attacks:** Attackers capture legitimate RF transmissions (e.g., remote keyless entry, garage openers, industrial remote control commands) and re-transmit them later to gain unauthorized physical or operational access.
- **GPS/Signal Spoofing:** In transportation, logistics, and maritime industries, malicious RF transmitters can spoof GPS signals or positioning telemetry to disrupt navigation systems or trick automated machinery. Monitoring signal strength, arrival angles, and power levels helps flag spoofed signals.



5. Securing IoT, Medical, and OT Environments

Many Internet of Things (IoT) sensors, medical devices, and industrial SCADA components lack the computational power or memory required to run local encryption protocols, EDR agents, or heavy security software.

- **Agentless Monitoring:** Because security software cannot be installed directly on low-power devices, RF monitoring acts as an external, passive security layer.
- **Behavioral Baseline:** By analyzing the RF emissions of lightweight devices (transmission frequency, timing, and power), security systems can detect abnormal behavior indicative of device tampering or firmware exploitation.



Summary

Without RF level monitoring, an organization's cybersecurity perimeter ends at its network cables and managed access points. Integrating physical spectrum monitoring into broader Security Information and Event Management (SIEM) workflows ensures complete, end-to-end visibility across both digital and physical domains. Contact Saelig for more information about [RadGreen's RF Cybersecurity solutions](#): salesmgr@saelig.com or 585-385-1750.

