**🔐 PROTECTION DEFENSES FOR WIRELESS COMMUNICATION**

**✅ 1. Wi-Fi Protection Defenses**

**📡 Threats Wi-Fi Faces:**

* Packet sniffing
* Rogue Access Points (Evil Twin)
* WPA/WPA2 handshake cracking
* Deauthentication attacks
* Man-in-the-Middle (MITM)
* Weak password brute force

**🔐 Recommended Defenses:**

| **Category** | **Defense Strategy** | **Tools / Actions** |
| --- | --- | --- |
| **Encryption** | Use **WPA3** encryption | WPA3 > WPA2 > WPA (avoid WEP) |
| **Authentication** | Enable **802.1X** with RADIUS | For enterprise networks |
| **Strong Passwords** | Use **strong PSKs**, avoid dictionary words | Use tools like diceware |
| **MAC Filtering** | Allow only known device MAC addresses | Not foolproof, can be spoofed |
| **Disable WPS** | WPS is easily brute-forced | Turn it off in router settings |
| **Hide SSID** | Prevent casual discovery | But not a strong defense |
| **Access Point Isolation** | Prevents client-to-client attack | Enable in router settings |
| **Network Segmentation** | Use VLANs for IoT vs admin vs guest | Isolate untrusted devices |
| **Deauth Protection** | Monitor with **WIDS** | Use tools like Kismet or AirDefense |
| **Firmware Updates** | Update routers/access points | Fixes known vulnerabilities |

**🔁 Bonus Tip: Rotate PSK every 90 days and log Wi-Fi authentication attempts.**

**🚫 2. Non-Wi-Fi Protocols (RF, Bluetooth, IR, Zigbee, etc.)**

These include **Bluetooth, Zigbee, RF remotes, RFID, NFC, LoRa**, and more — all used in **IoT devices**, **industrial controls**, and **consumer electronics**.

**🔍 Common Threats:**

* Replay attacks
* Sniffing (unencrypted comms)
* Signal jamming
* Device spoofing
* Unauthorized pairing

**🔐 Recommended Defenses:**

| **Protocol** | **Defense Strategy** | **Explanation** |
| --- | --- | --- |
| **Bluetooth** | Use **Bluetooth 5+**, turn off when unused | Enforce **authentication + encryption** |
| **RF 433/868 MHz** | Use **rolling codes** (e.g., in car remotes) | Avoid fixed-code systems |
| **Zigbee** | Enable **network key encryption** | Use trust center link key |
| **IR (Infrared)** | Line-of-sight, so limit exposure | Shield IR receivers |
| **NFC** | Keep range limited (<4cm), use **tokens** | NFC can be skimmed |
| **RFID** | Use **Faraday sleeves**, secure access control systems | RFID tags can be cloned |
| **LoRaWAN** | Enforce **end-to-end AES encryption** | Often used in long-range IoT |
| **DECT Phones** | Use encrypted base stations | Don’t leave on default config |

**🔐 Tools for Monitoring/Defense:**

* **Bastille**: Detects rogue RF signals & anomalies
* **RFIDler** / **Proxmark3**: For testing RFID/NFC defenses
* **Bluetooth Analyzer**: See active Bluetooth devices
* **SDR (HackRF, RTL-SDR)**: Visualize RF spectrum, detect jamming

**🧠 Network Defense Mindset:**

"The more invisible and silent the protocol, the more important it is to **monitor, segment, and lock it down**."

**📌 Summary Table**

| **Protocol Type** | **Best Defense** |
| --- | --- |
| **Wi-Fi** | WPA3 + VLAN + 802.1X + Deauth protection |
| **Bluetooth** | Turn off when unused, pair only trusted |
| **RFID/NFC** | Use shields, limit range, rotate access keys |
| **Zigbee/LoRa** | Enable encryption + use secure join mechanisms |
| **Infrared** | Physical shielding, no confidential data |
| **RF** | Avoid fixed codes, use frequency hopping |