**🔍 Non-WiFi Wireless Technologies – Quick Review (Hacking 101)**

**🧠 Why Learn This?**

While Wi-Fi is common, attackers often **exploit other wireless tech** that people forget about. These can be **entry points** into networks, smart devices, or even physical security systems.

**📡 Common Non-WiFi Wireless Technologies:**

**1. Bluetooth**

* **Range**: ~10–100 meters
* **Use Cases**: Headphones, car audio, keyboards, smart devices
* **Attacks**:
  + **Bluejacking** – Send unsolicited messages
  + **Bluesnarfing** – Access data on device
  + **Bluebugging** – Take full control

🔧 Tools: bluesniff, blueranger, hcitool, ubertooth

**2. ZigBee**

* **Used in**: Smart homes (lights, locks), IoT sensors
* **Weakness**: Weak encryption, often poorly implemented
* **Attacks**: Hijack devices, inject commands

🔧 Tools: KillerBee (ZigBee sniffer & injector)

**3. RFID/NFC (Radio Frequency Identification / Near-Field Communication)**

* **Use in**: Access cards, metro cards, credit cards, passports
* **Attacks**:
  + **Skimming** – Read data remotely
  + **Cloning** – Duplicate an RFID/NFC card
  + **Eavesdropping** – Intercept communication

🔧 Tools: Proxmark3, ChameleonMini, ACR122U, mobile apps (Android NFC)

**4. LoRa/LoRaWAN (Long Range)**

* **Use**: Low-power sensors in agriculture, factories, cities
* **Security Flaws**: Often lacks encryption, replay protection
* **Risk**: Can spoof or flood LoRa devices/networks

🔧 Tools: LoRa Sniffer, SDR (Software-Defined Radio)

**5. Z-Wave**

* **Use in**: Home automation (like ZigBee)
* **Attacks**:
  + Replay attacks
  + Downgrade encryption
  + Jamming

🔧 Tools: USB dongles + Z-Wave Sniffer, OpenZWave

**6. Infrared (IR)**

* **Use**: TV remotes, security cameras, some laptops
* **Vulnerability**: Can be intercepted, replayed
* **Tools**: LIRC, IR LEDs with Raspberry Pi or Arduino

**7. Cellular (GSM/3G/4G/5G)**

* **Risks**:
  + **IMSI Catchers** (fake cell towers)
  + **SMS spoofing**
  + **Call interception**

🔧 Tools: OpenBTS, YateBTS, Osmocom, SDRs like HackRF

**8. Satellite Communication**

* **Use in**: Remote industries, ships, military, TV
* **Vulnerability**: Unencrypted data streams, weak auth
* **Tools**: SDR, Skywave, satellite dish setups

**9. DECT (Digital Enhanced Cordless Telecommunications)**

* **Use**: Old cordless phones
* **Attacks**: Eavesdropping, call interception

🔧 Tools: DECT Sniffer, Com-On-Air cards

**🧰 Tools to Explore Multiple Wireless Techs:**

* **HackRF One** (SDR – Software Defined Radio)
* **Ubertooth One** (Bluetooth)
* **Proxmark3** (RFID/NFC)
* **RTL-SDR** (General radio signals)
* **Flipper Zero** (multi-protocol pentesting device)

**🧠 Summary Table**

| **Tech** | **Attack Surface** | **Tools** |
| --- | --- | --- |
| Bluetooth | Device control | Ubertooth, hcitool |
| ZigBee | IoT Devices | KillerBee |
| RFID/NFC | Access Cards | Proxmark3 |
| LoRa | Remote sensors | SDR, LoRa sniffer |
| Z-Wave | Smart Homes | OpenZWave |
| IR | Replay signals | LIRC, Pi IR setups |
| GSM/4G | Calls/SMS | OpenBTS, SDR |
| Satellite | Data interception | Skywave, SDR |