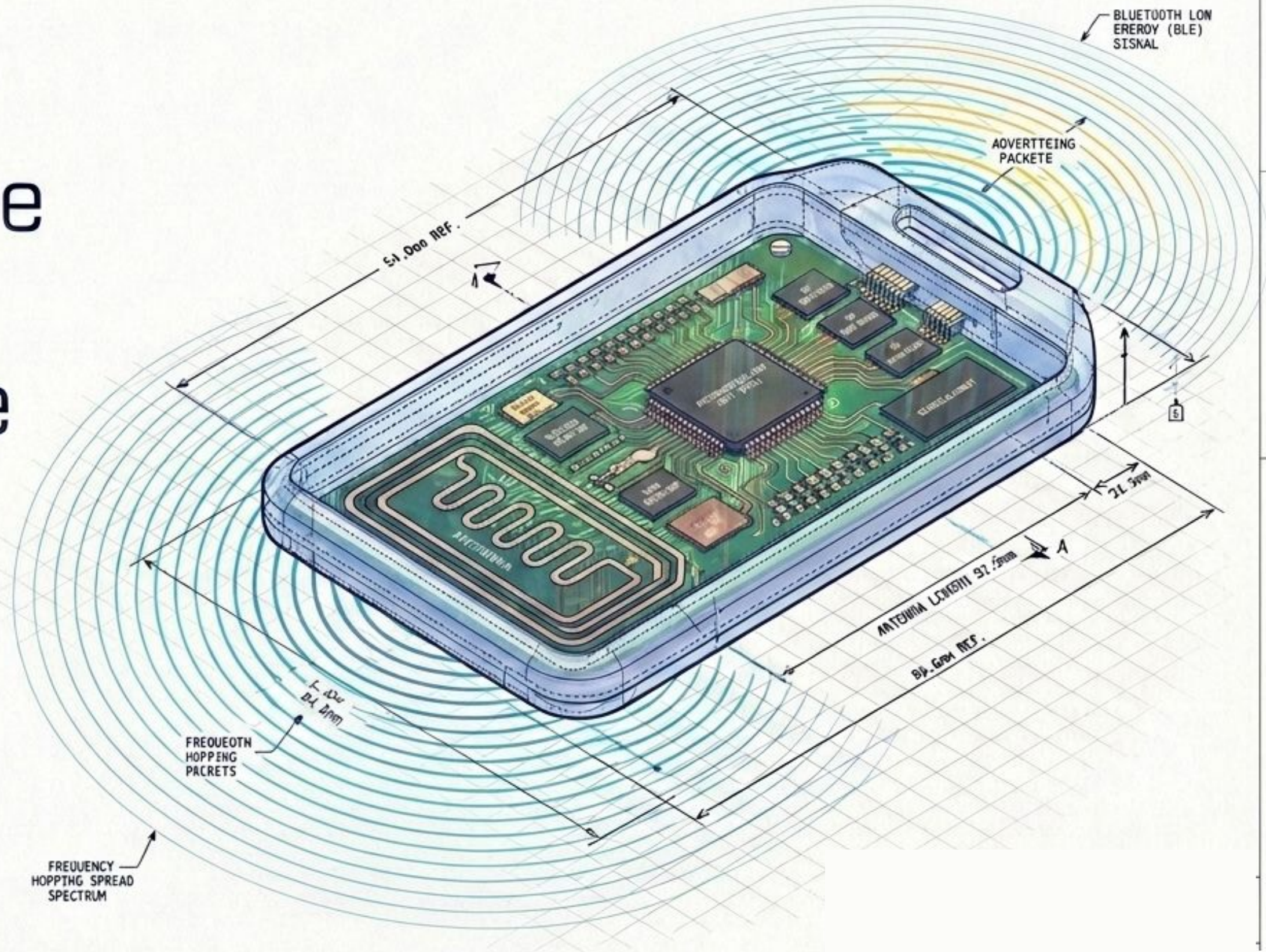


Illuminating the Bluetooth Attack Surface

A Practical Primer for Security Teams



The Wireless Visibility Gap

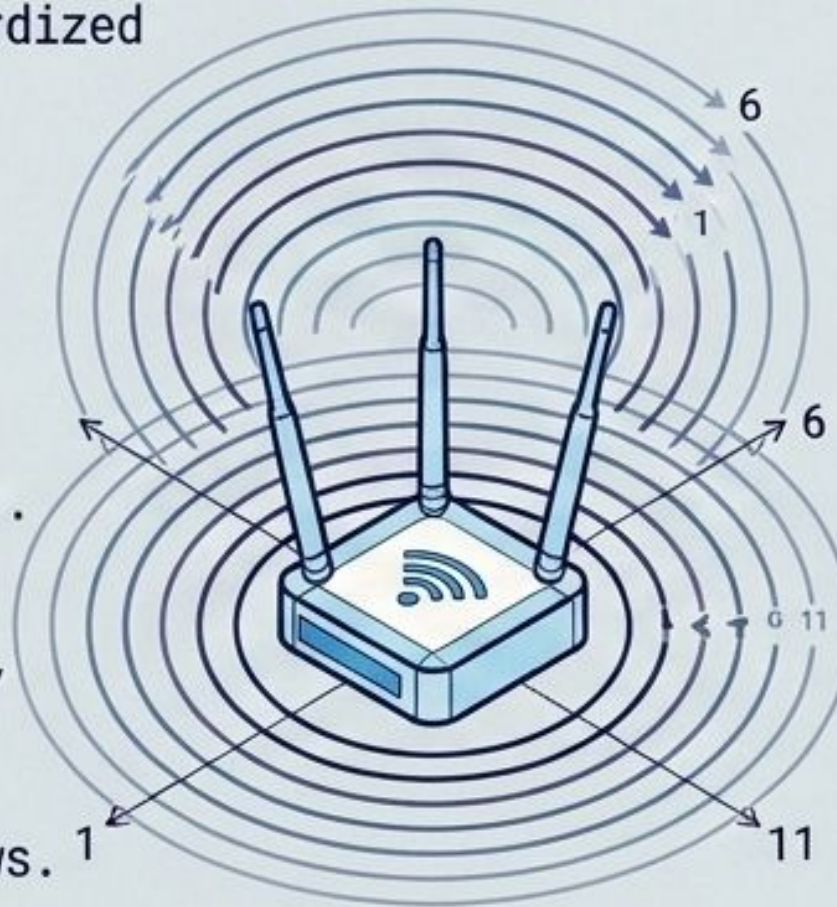
Bluetooth and Wi-Fi both launched in 1999, yet defenders treat one as a transparent standard and the other as a mysterious black box.

Wi-Fi Security (The Glass Box)

- ✦ **Concepts:** WPA encryption, standardized packet capture, standard AP configuration.

- ✦ **Spectrum:** 3 predictable, non-overlapping channels (1, 6, 11).

- ✦ **Visibility:** High. Supported by widely available adapters and familiar enterprise workflows.

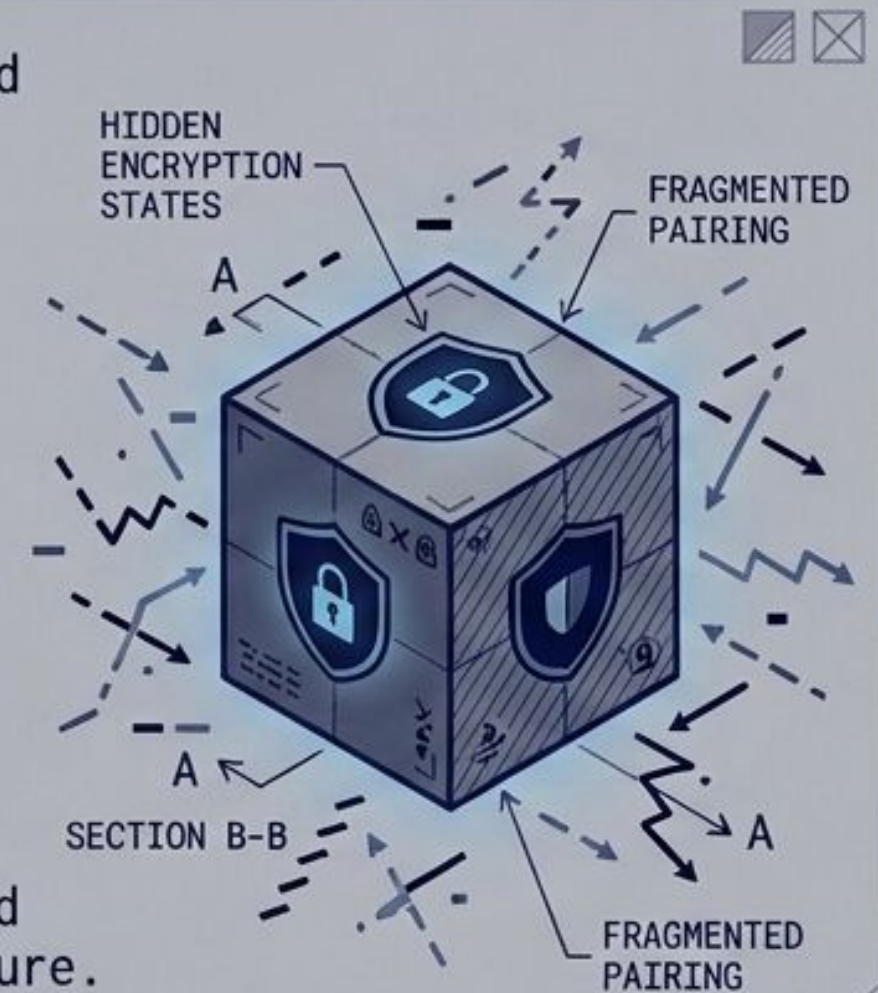


Bluetooth Security (The Black Box)

- ✦ **Concepts:** Fragmented pairing methods, hidden encryption states, multiple protocol stacks.

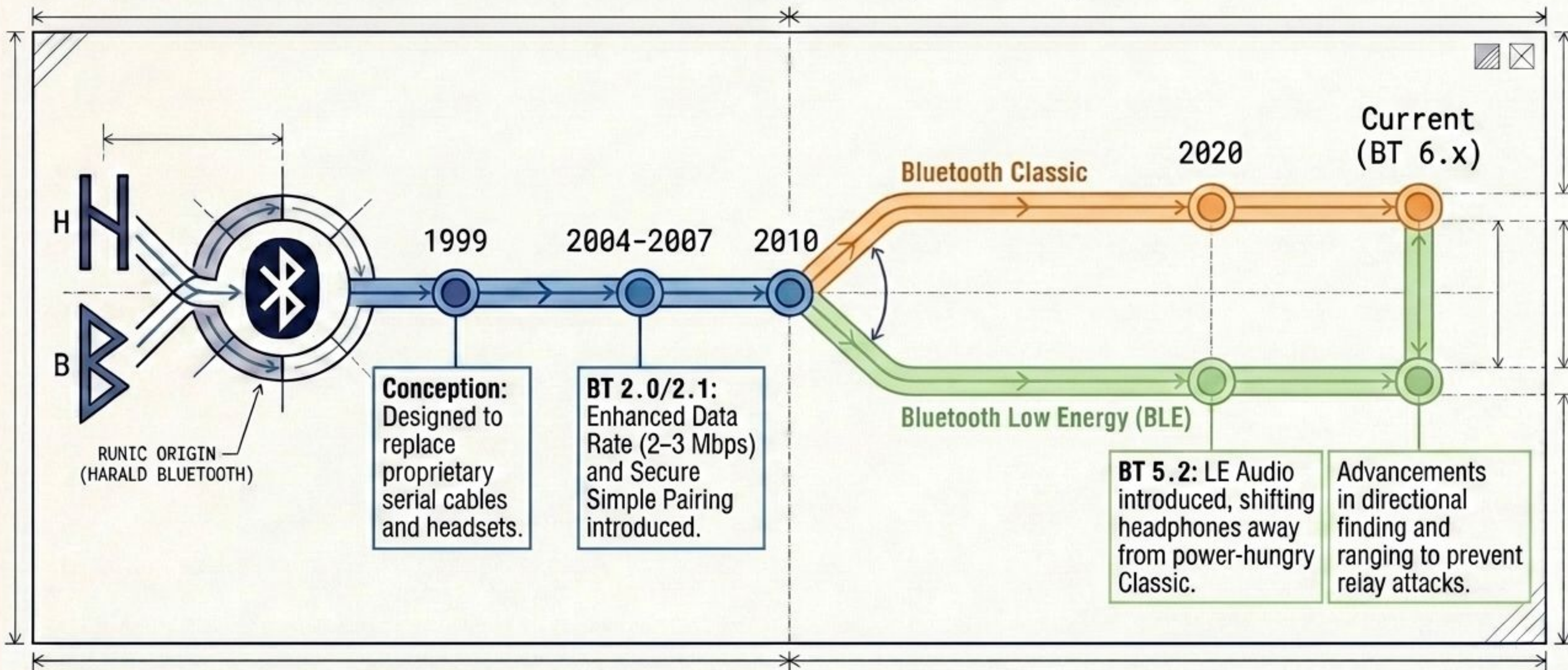
- ✦ **Spectrum:** Rapid frequency hopping across up to 79 distinct channels.

- ✦ **Visibility:** Low. OS hides version/encryption; requires specialized tools to fully capture.



The Evolution of Bluetooth

Named after 10th-century Danish King Harald Bluetooth Gormsson, the protocol was designed to unite disconnected devices—evolving rapidly over 25 years.



The Dual Stack Framework

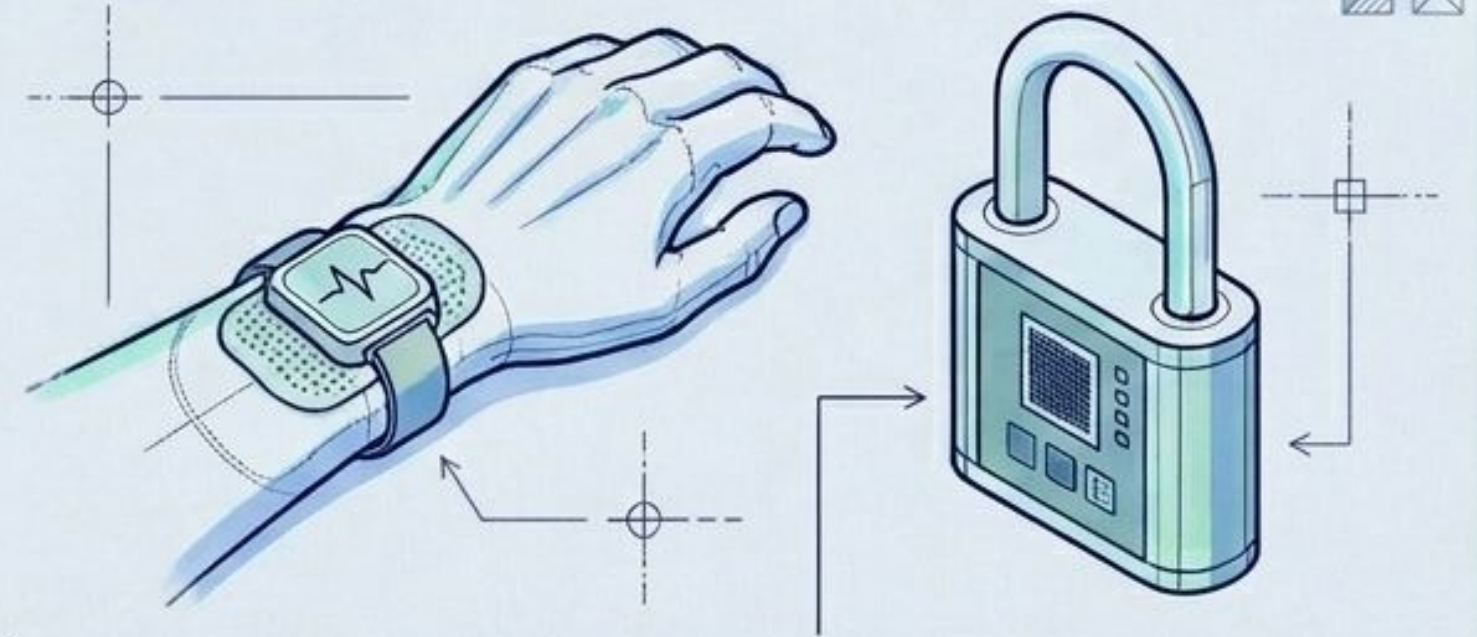
Modern Bluetooth encompasses two parallel architectures tailored for completely different physical requirements.

Bluetooth Classic (BR/EDR)



- ⊕ **Primary Goal:** Continuous communication and high-throughput data streaming.
- ⊕ **Power Profile:** Power hungry (radio wakes frequently).
- ⊕ **Spectrum:** 79 channels.
- ⊕ **Target Devices:** Older vehicles, traditional headsets, continuous audio streaming.

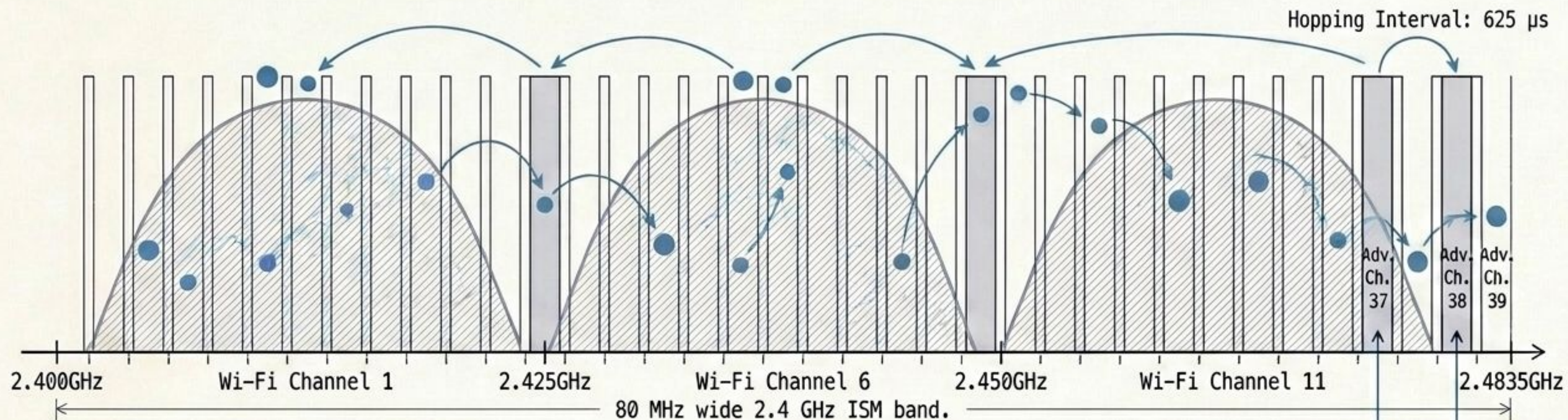
Bluetooth Low Energy (BLE)



- ⊕ **Primary Goal:** Occasional short bursts of data.
- ⊕ **Power Profile:** Extreme efficiency (radio sleeps up to 99% of the time; runs on coin cells for years).
- ⊕ **Spectrum:** 40 channels.
- ⊕ **Target Devices:** Wearables, medical sensors, asset trackers, smart locks.

Evasion by Design in the 2.4 GHz Band

Bluetooth's rapid channel-switching ensures reliability against collisions, but creates a massive hurdle for continuous security monitoring.

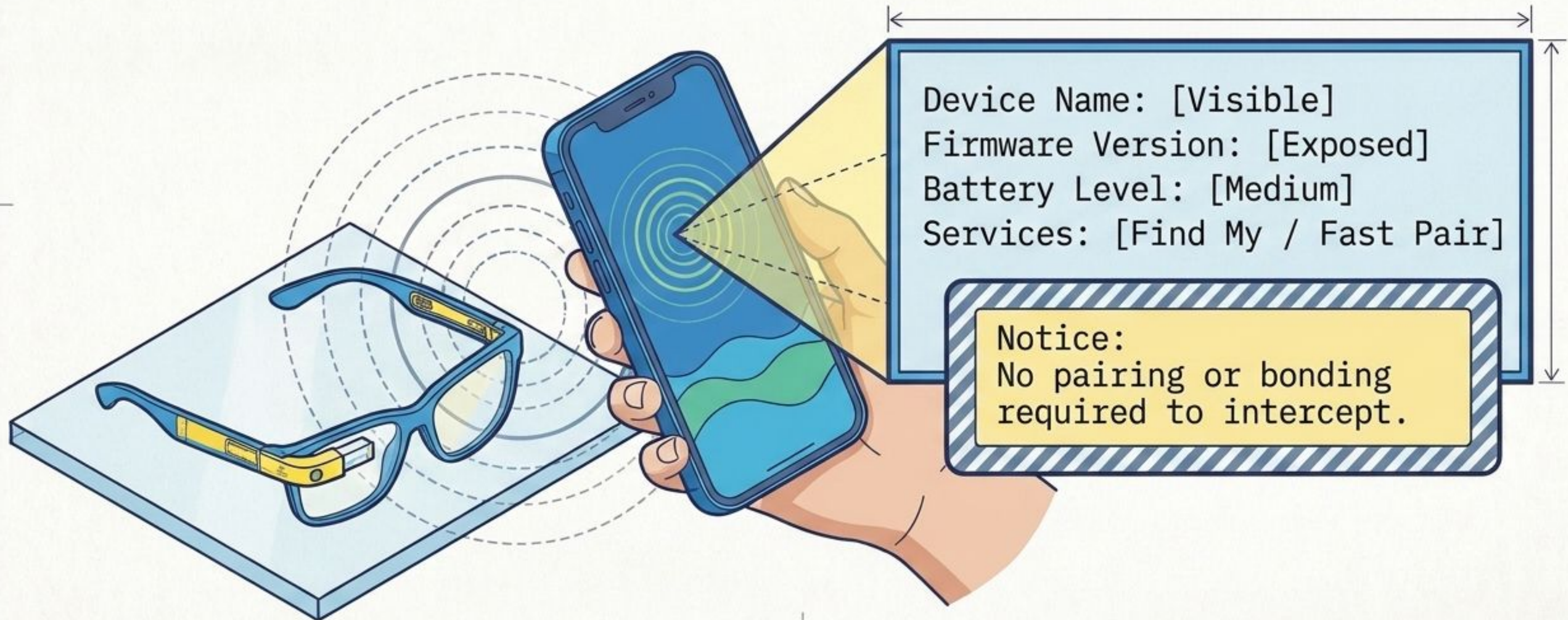


Adaptive Frequency Hopping

- maps out interference and actively avoids the static Wi-Fi channels. 3 dedicated advertising channels explicitly sit in the empty gaps between Wi-Fi channels.

The Exposed Advertising Layer

BLE devices constantly broadcast their presence to be discovered.
Poor implementations leak sensitive metadata to anyone listening.



The Connection Escalation Staircase

3. Bonding

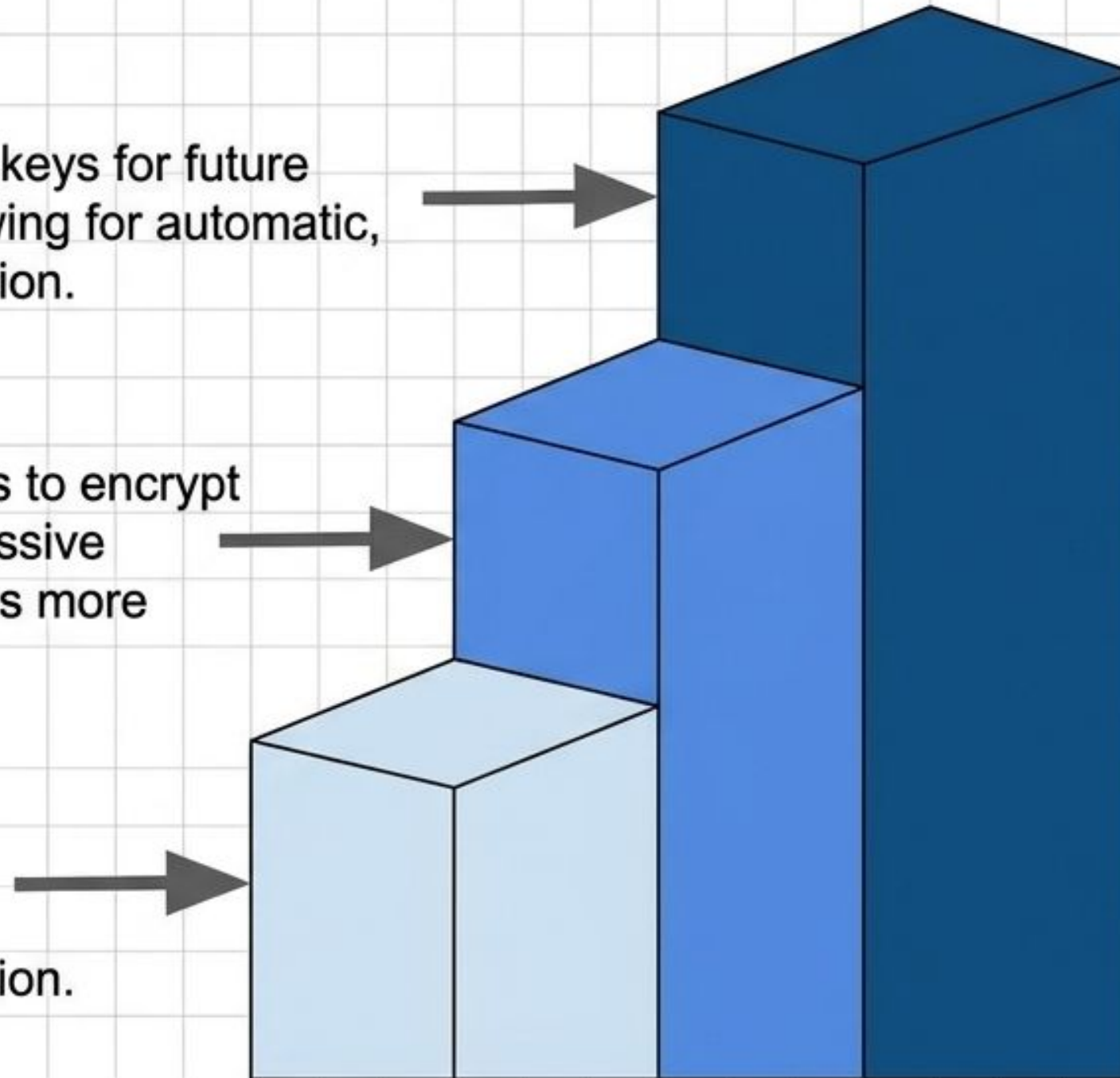
Store the security keys for future connections, allowing for automatic, secure re-connection.

2. Pairing

Exchange security keys to encrypt the link and prevent passive eavesdropping. Enables more services.

1. Connecting

Establish a basic, unencrypted link for temporary communication. Limited functionality.

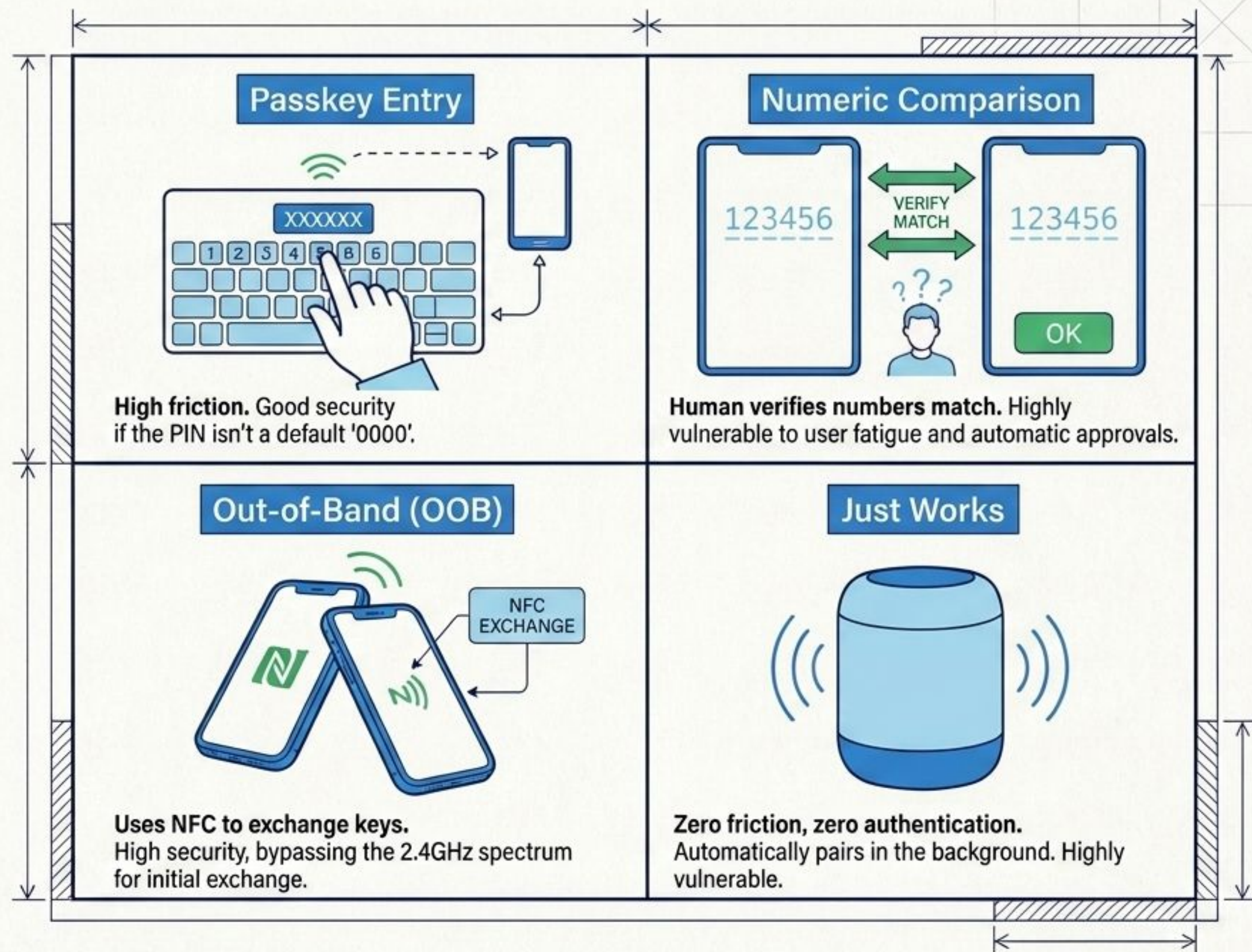


Risk Annotation

- Each step increases the level of access and potential risk.
- **Connecting:** Low risk, transient exposure.
- **Pairing:** Medium risk, vulnerable to MITM during key exchange.
- **Bonding:** High risk, persistent access if keys are compromised.

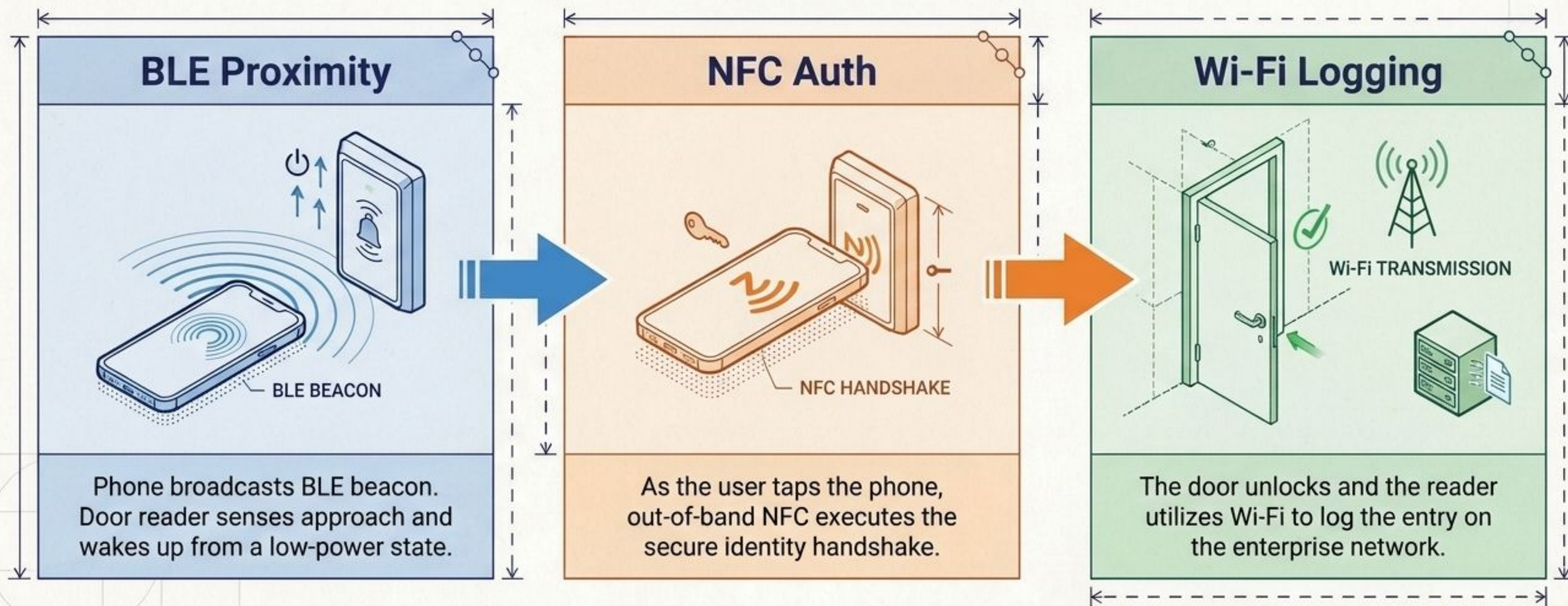
Negotiating Trust: The Four Pairing Methods

Security protocols trade cryptographic strength for user convenience, relying on human verification to prevent man-in-the-middle attacks.



Synthesis: The Multi-Protocol Kill Chain

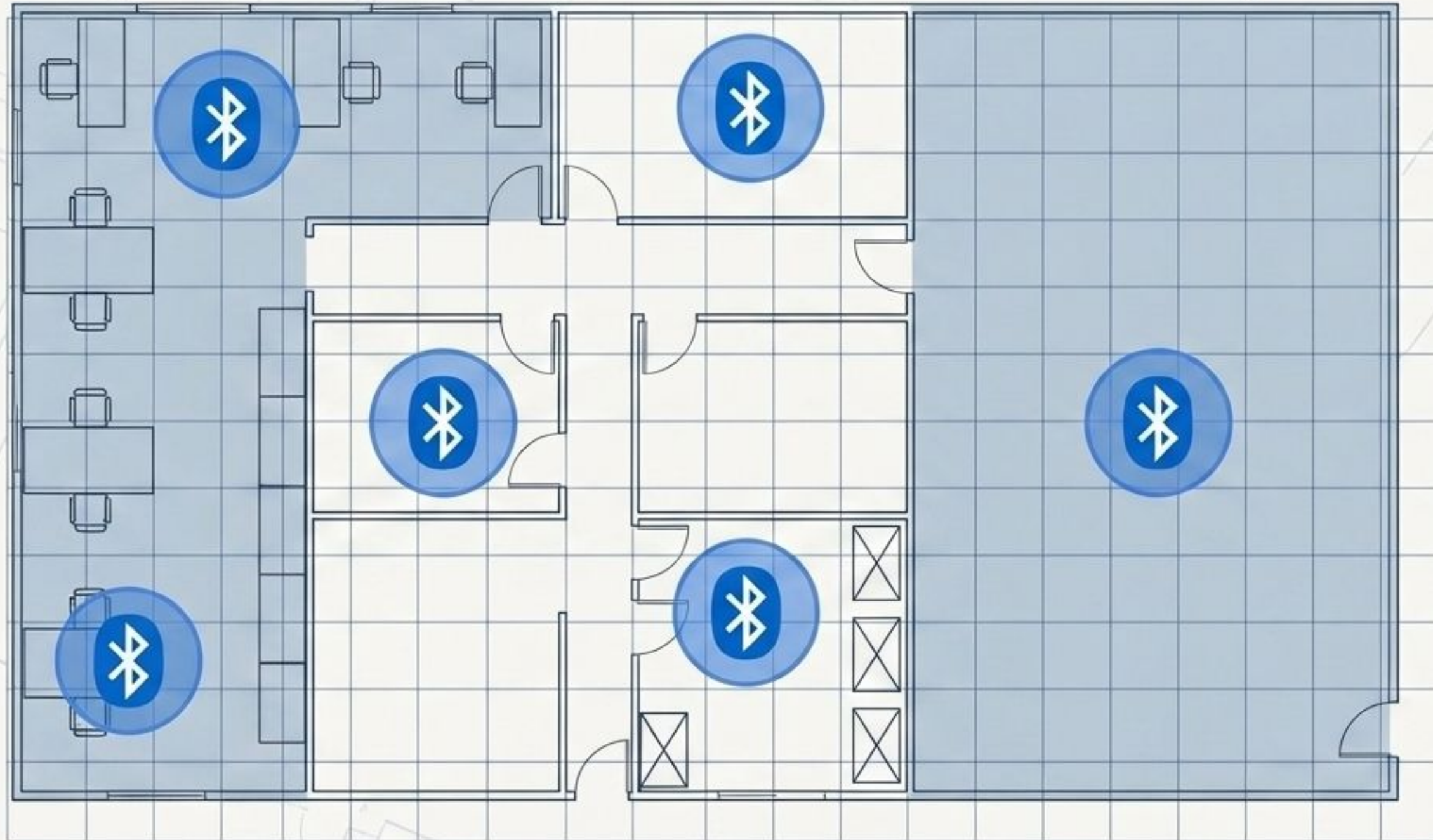
Bluetooth is the connective tissue of modern workflows. Compromising it often yields access to Wi-Fi, cellular, or physical security systems.



Corporate

Healthcare/Safety

Industrial

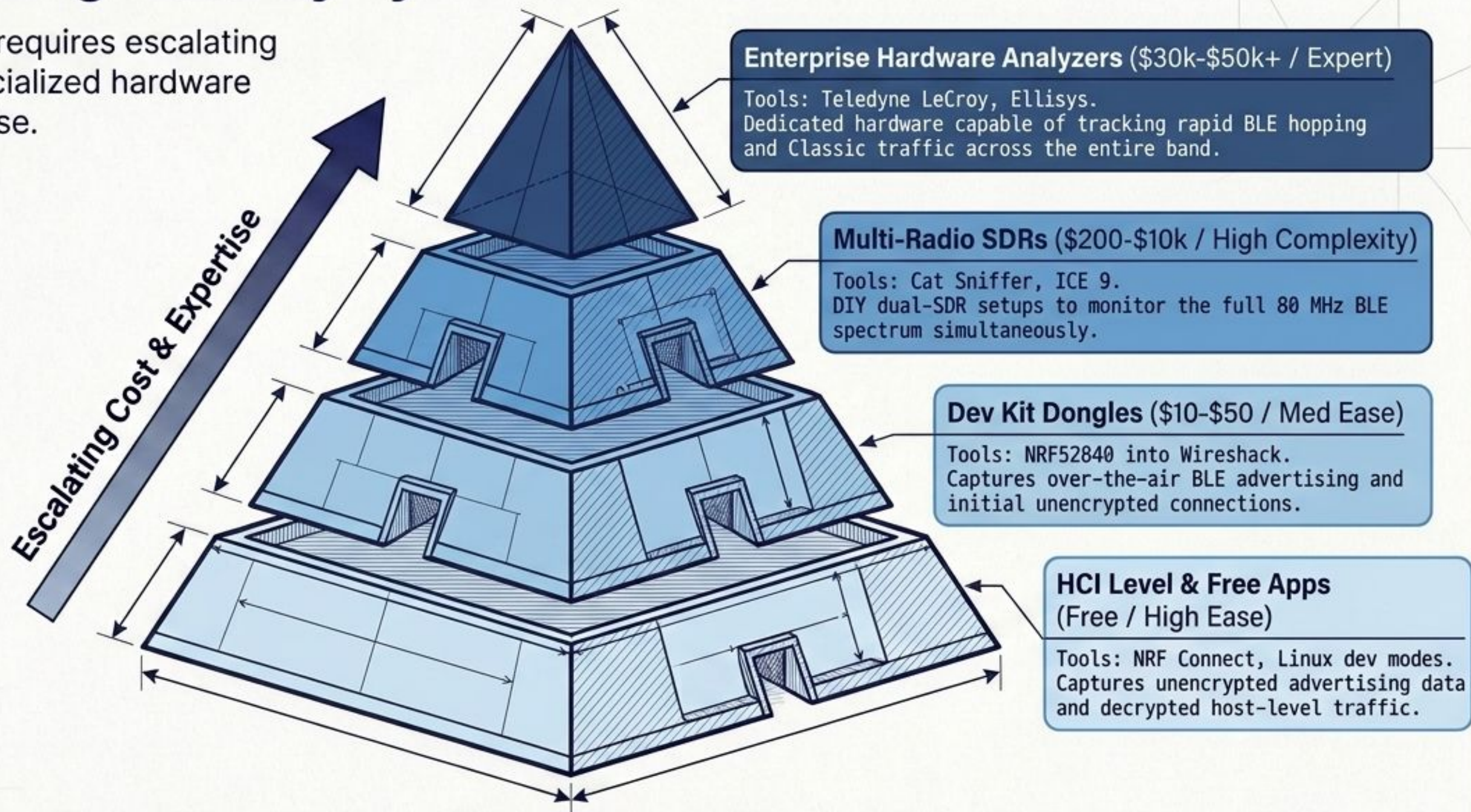


Key Takeaway

Bluetooth devices are now present across corporate, healthcare, and industrial environments, converging in modern facilities.

The Monitoring Maturity Pyramid

Regaining visibility requires escalating investments in specialized hardware and analyst expertise.



The Vendor Evaluation Scorecard

A Bluetooth version number (e.g., 'BT 6.0') is merely a marketing claim.
True enterprise security must be evaluated through implementation quality.

Red Flags (Indicators of Compromise)	Green Flags (Enterprise Readiness)
 Uses outdated Secure Simple Pairing (BT 2.1 era) on modern devices.	 Official Bluetooth SIG Certification status (verifies compliance with BT 4.2+ secure connection standards).
 Relies entirely on 'Just Works' pairing for sensitive data transfers.	 Verifiable firmware update process specifically for the radio controller.
 Exposes unnecessary diagnostic services (battery, firmware) prior to authentication.	 Integration with enterprise manageability and MDM workflows.

Closing the Visibility Gap

Bluetooth is no longer an isolated protocol for short cables. It is a quantifiable, omnipresent attack surface demanding integration into standard security workflows.

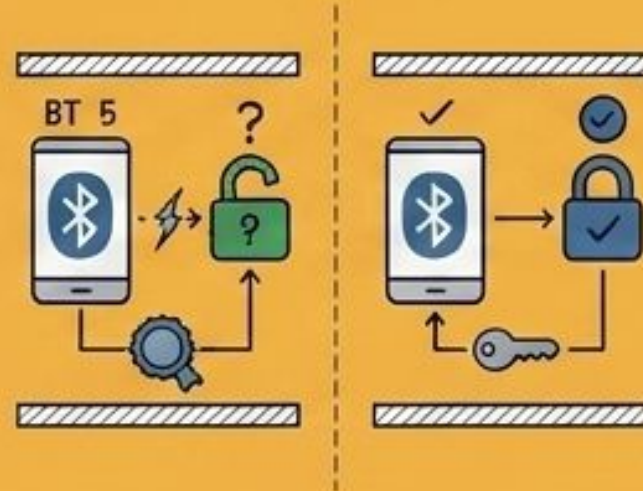
1. Inventory

Map all Bluetooth-capable assets across physical security systems, IoT, and standard IT.



2. Validate

Test hardware vendor claims. Do not assume "Bluetooth 5" implies modern encryption is active.



3. Monitor

Deploy localized sniffing in highly sensitive zones (executive spaces, industrial muster points) to detect unauthorized bonding.

