# 6.7 Bluetooth Security

## Legacy Pairing vs. LE Secure Connections

Pairing is the process of creating a trusted relationship between two devices by generating and storing shared secret keys.

- **Legacy Pairing:** Used in Bluetooth versions prior to 4.2. While it provided security, certain association models (like "Just Works") were vulnerable to passive eavesdropping and Man-in-the-Middle (MITM) attacks because they did not authenticate the user or device.
- **LE Secure Connections:** The modern security standard for BLE. It is a significantly more robust pairing method that uses a government-grade cryptographic algorithm called **Elliptic Curve Diffie-Hellman (ECDH)** for key exchange. This algorithm provides a very high level of protection against passive eavesdropping, even if an attacker manages to capture all the pairing packets. LE Secure Connections is the mandatory security foundation for modern BLE devices.

## Encryption, Privacy, and MITM Protection

Modern Bluetooth security is built on three core pillars:

1. **Encryption (Confidentiality):** Once devices are paired, the connection can be encrypted. Bluetooth uses the **AES-CCM** algorithm to encrypt all data sent over the link. This ensures that if an attacker were to listen to the radio traffic, they would only see unintelligible encrypted data, not the actual information.
2. **Privacy (Anti-Tracking):** To prevent malicious actors from tracking a user by listening for their device's Bluetooth address, BLE uses **Resolvable Private Addresses (RPAs)**. A device with this feature enabled will periodically change its public Bluetooth address to a new, randomized one. Only devices that have previously paired with it possess the key (the IRK - Identity Resolving Key) needed to resolve this random address and identify the device.
3. **Authentication and MITM Protection:** A Man-in-the-Middle (MITM) attack occurs when an attacker secretly sits between two devices and relays their communication, potentially altering it. LE Secure Connections protects against this by authenticating the connection during pairing. This is done using one of several association models:
   - **Passkey Entry:** The user enters a 6-digit number on both devices.
   - **Numeric Comparison:** A 6-digit number is displayed on both devices, and the user confirms they are the same. This is the most common method for devices with displays.

- If a connection is authenticated, the devices have proven they are communicating directly with each other and not an imposter.

# Security Best Practices for Developers

For students building Bluetooth applications, security should be a primary concern.

- **Use LE Secure Connections:** Always use the highest security mode available on your platform. Avoid legacy pairing if possible.
- **Authenticate When Possible:** For devices with a display or keyboard, use Numeric Comparison or Passkey Entry to protect against MITM attacks. For devices without a user interface (like a sensor), you must be aware that the connection is unauthenticated.
- **Enable Privacy:** Use Resolvable Private Addresses to prevent your device from being tracked over time.
- **Validate Data:** Do not blindly trust the data received over a BLE link. Always validate it at the application layer to ensure it is in the expected format and range.
- **Use the Correct Security Level for Characteristics:** Define the minimum security level (encryption, authentication) required to read or write specific GATT characteristics. Don't expose sensitive data on an open, unencrypted connection.

---

Revision #1
Created 2025-08-28 11:53:00 UTC by GI
Updated 2025-08-28 12:19:33 UTC by GI