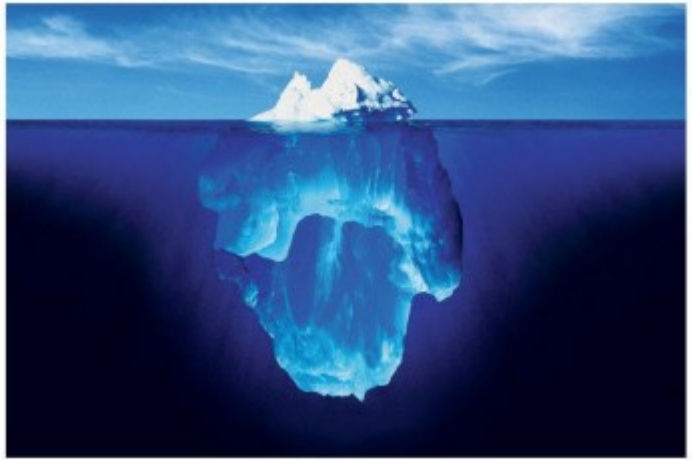
BLE Security Fundamentals

Embedded Systems Design Team
C-DAC Hyderabad
by
C.MAHESH

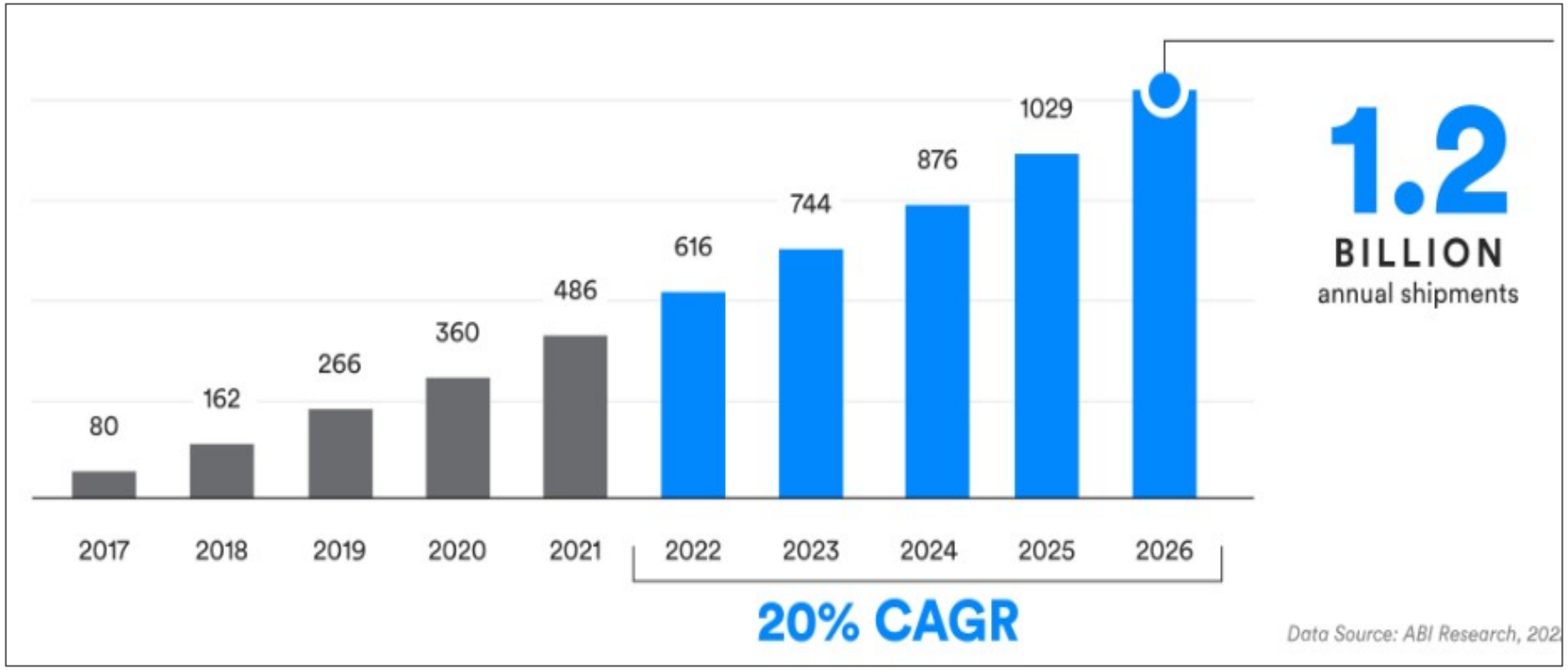
Agenda

- *Basics of BLE (Tip of the iceberg)*
- *Attack*
- *BLE Security*
- *Recommendation*



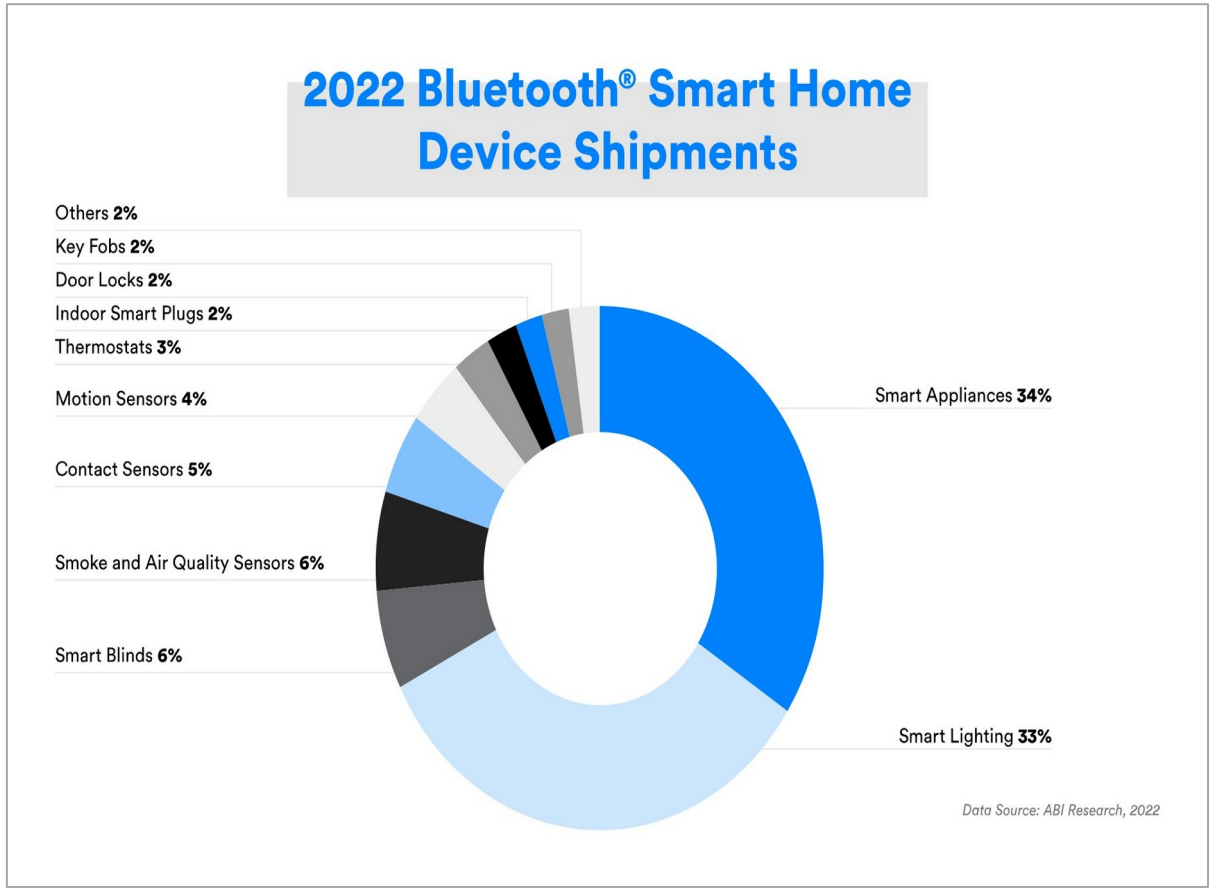
Why Will Talk About Bluetooth?

Bluetooth device Network device shipments



Bluetooth Smart Home Device Shipments :

Smart Home Device Shipments



What is BLE(Bluetooth Low Energy) ?

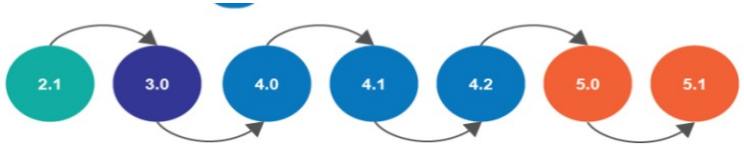
- Wireless technology standard, designed from ground up.
- ***What is the meaning of "Low" in "Bluetooth Low Energy" ...?***
  - Lower complexity
  - Lower power consumption / duty cycles
  - Short range communication
  - Lower data rates

- Frequency: Operates at 2.4 GHz ISM (***Industrial Scientific Medical***) band.
  - Same as Wi-Fi & your microwave
  - **Frequency-hopping spread spectrum(FHSS).**
- Low cost and ease of implementation lead BLE to be widely used among IoT devices and applications
- Wearables,sensors light bulbs, medical devices, & many other smart-products.

What is data rate / data Throughput ?

- Data rate in Bluetooth refers to the speed at which data is transmitted between Bluetooth-enabled devices.
- It represents the amount of data that can be transferred per unit of time and is typically measured in

  bits per second (bps) or kilobits per second (Kbps).



What is frequency spectrum?

- The frequency spectrum in Bluetooth refers to the range of frequencies used by Bluetooth wireless technology to transmit data between devices. Bluetooth operates in the **2.4 GHz ISM** (Industrial, Scientific, and Medical) band, which is a globally available unlicensed radio frequency band.

What is Adaptive Frequency Hopping?

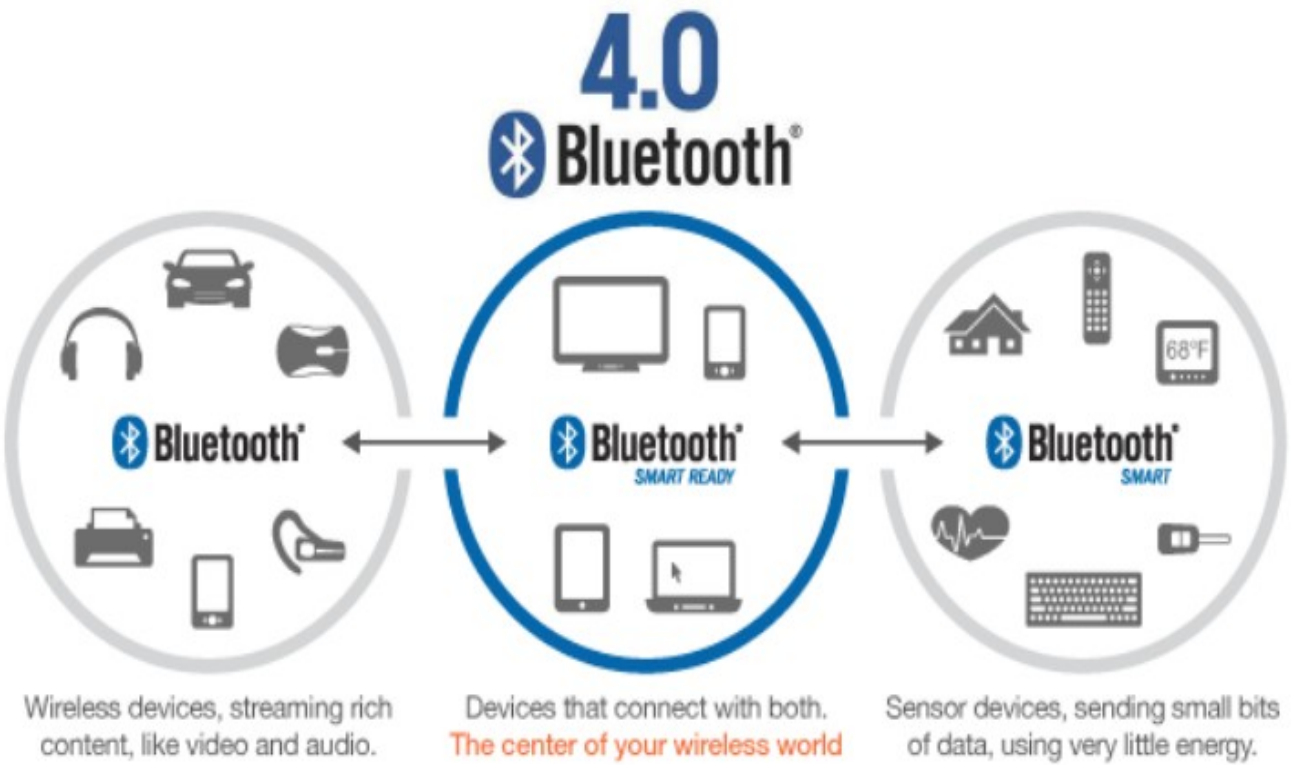
AFH allows Bluetooth devices to intelligently select and avoid channels that are experiencing interference, thus improving overall performance and reducing the likelihood of data collisions

- **Adaptive Frequency Hopping:** BLE uses frequency hopping to avoid interference with other wireless devices, but it does so in a way that adapts to the surrounding radio environment, thereby optimizing power consumption.
- To mitigate interference and ensure reliable communication, Bluetooth uses **Adaptive Frequency Hopping (AFH)** technique.

Note on Naming

SIG: BLE developed by SIG

- Bluetooth 4.0
- Bluetooth Low Energy
  - BLE, BTLE, LE
- SIG Preferred
  - Bluetooth Smart
  - Bluetooth Smart Ready



BLE Roles:

Master

Client

Can read/write data to Slave/Server

Central

Peripheral

Slave

Server

Has read/write data

Can receive broadcast data

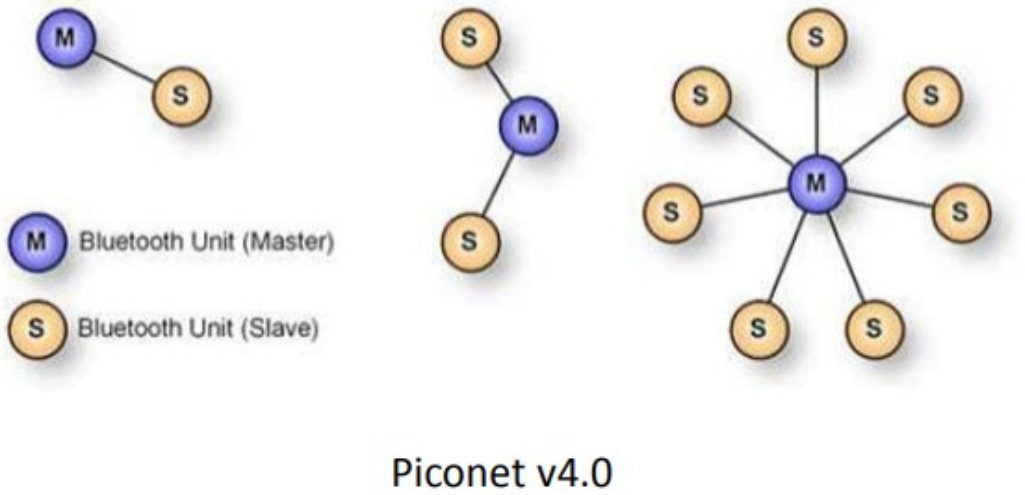
Observer

Broadcaster

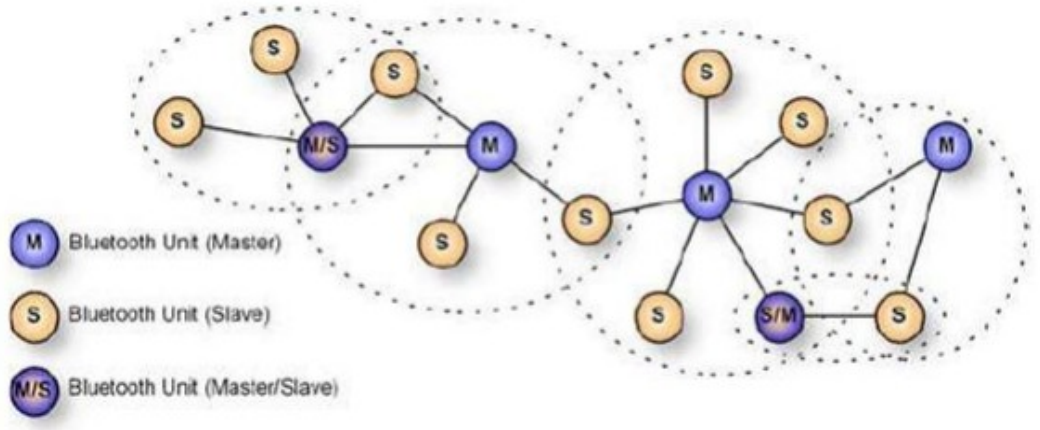
Has read-only broadcast

Topology:

Piconet & Scatter net: *(The multiple piocnet called as Scatter net)*



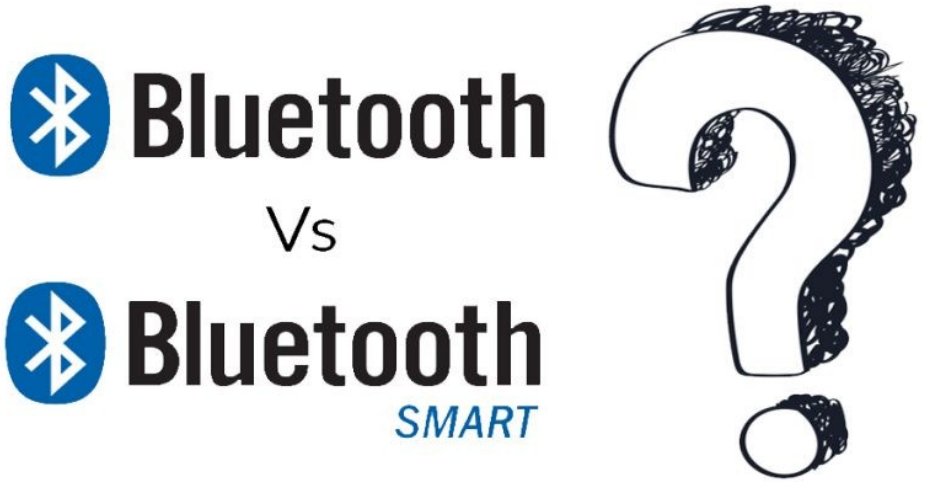
Piconet v4.0



Scatter net v4.1

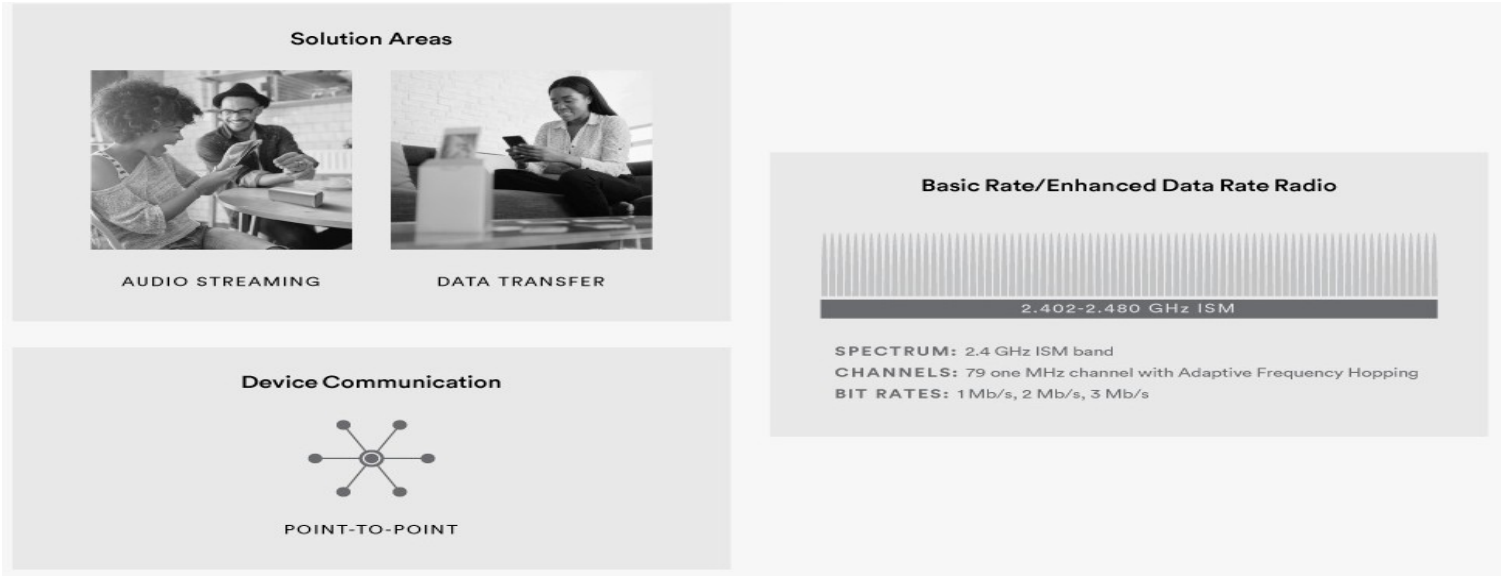
BLE vs BT Classic

- Different Architecture
- Different modulation parameter
- Different channel
- Different channel-hopping scheme
- Different packet format



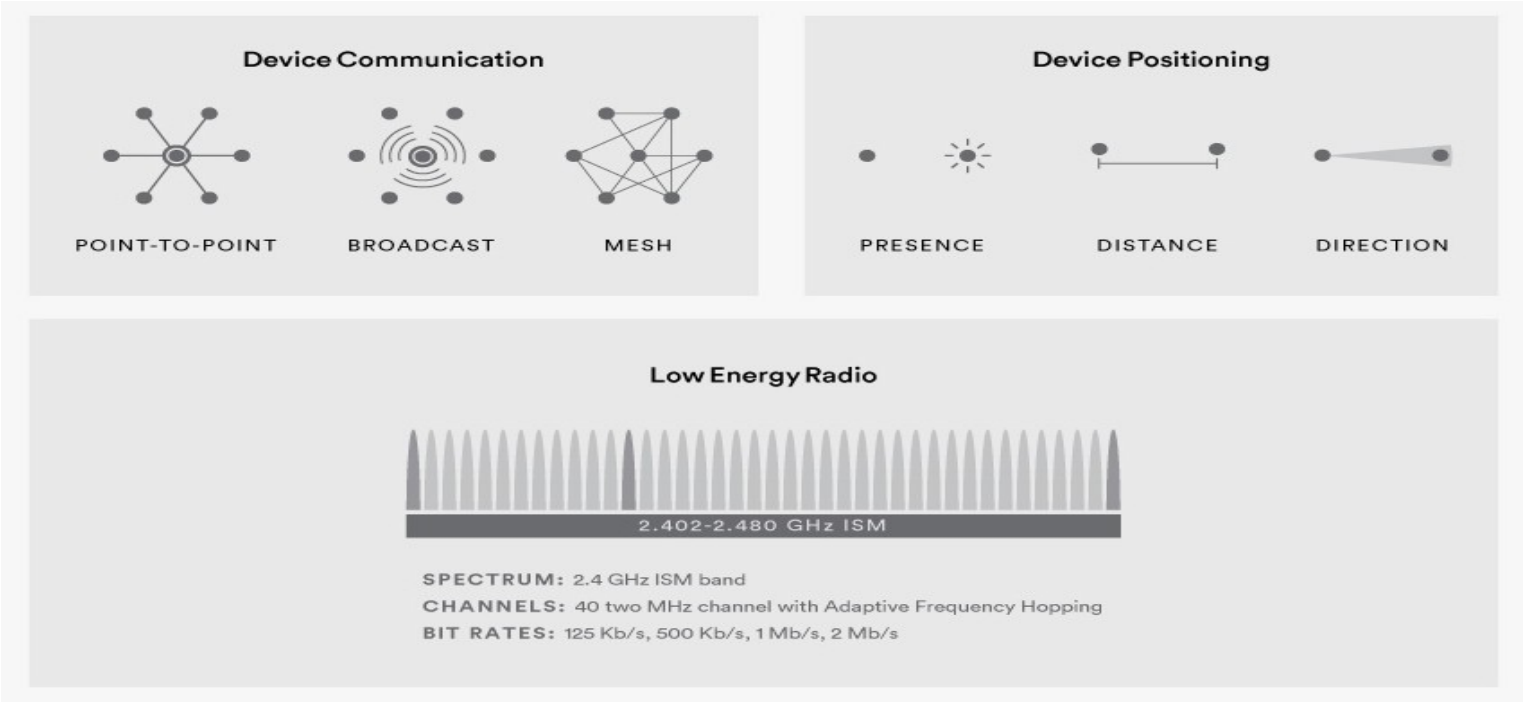
Classic Bluetooth:

- Classic Bluetooth is the original version of Bluetooth technology that was first introduced in 1999.
- It was designed for *high-bandwidth applications* such as streaming audio and video and supports devices with *higher power requirements*.
- Classic Bluetooth uses the *2.4 GHz ISM* (Industrial, Scientific, and Medical) band and has a maximum data rate of 3 Mbps.
- It has a range of up to *100 meters*, making it suitable for indoor and outdoor use. Classic Bluetooth devices can connect to other devices using a variety of protocols such as *A2DP (Advanced Audio Distribution Profile) for audio streaming and AVRCP (Audio/Video Remote Control Profile) for remote control of audio and video devices*.



Bluetooth Low Energy (BLE):

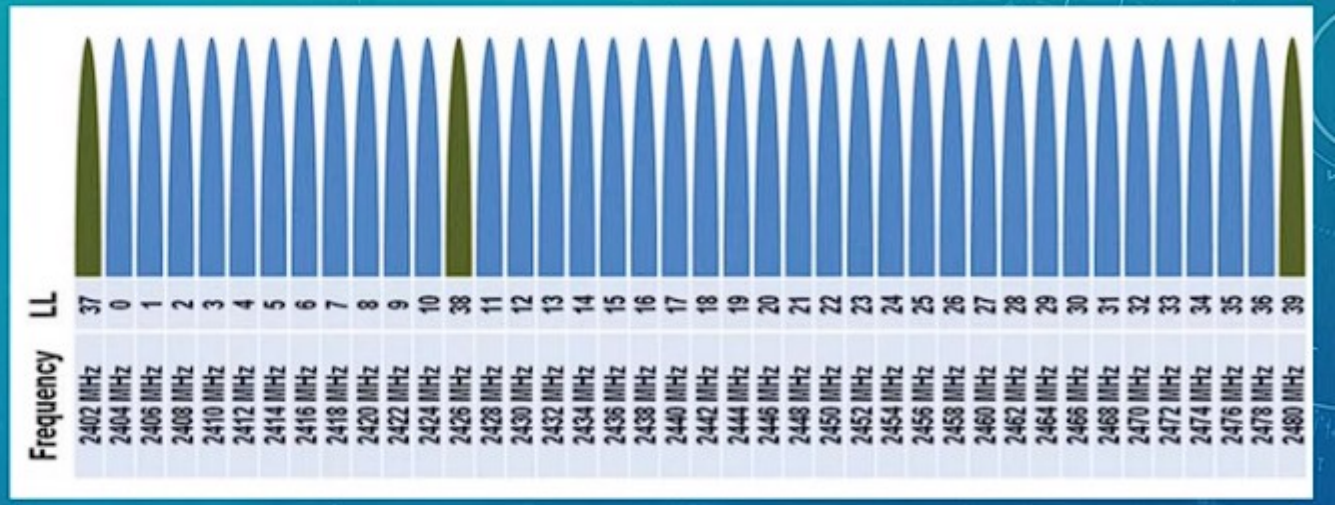
- BLE uses the same 2.4 GHz ISM band as Classic Bluetooth, but it has a lower power consumption and a shorter range.
- BLE devices can run on a coin cell battery for months or even years.
- BLE has a maximum data rate of 1 Mbps and a range of up to 50 meters.
- BLE devices can connect to other devices using a variety of protocols such as ***GATT (Generic Attribute Profile) for data exchange and GAP (Generic Access Profile)*** for device discovery and connection



Bluetooth Classic vs BLE

Bluetooth Classic	BLE
Used for streaming applications such as audio streaming, file transfers, and headsets	Used for sensor data, control of devices, and low-bandwidth applications
Not optimized for low power, but has a higher data rate (3Mbps maximum compared to 2Mbps for BLE)	Meant for low power, low duty data cycles
Operates over 79 RF (radio frequency) channels	Operates over 40 RF channels.
Discovery occurs on 32 channels	Discovery occurs on 3 channels, leading to quicker discovery and connections than Bluetooth Classic

CONTROLLER

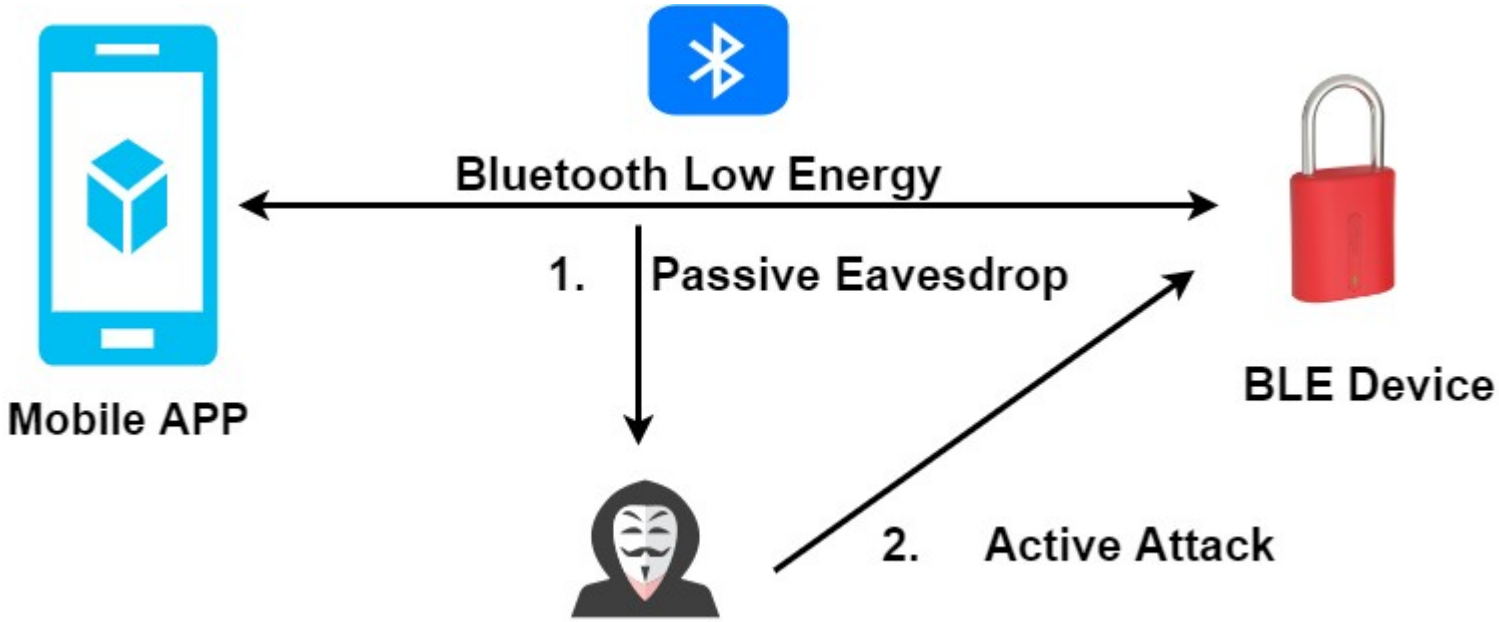


- **Physical Layer:**

- Modulation > GFSK (Gaussian Frequency Shift Keying)
- 2.4 GHz ISM Frequency band in range from 2.4000 GHz to 2.4835 GHz. Its an unlicensed band for industrial, scientific and medical uses.
- 2.4 GHz is divided into 40 RF Channels. (F = 2402 + k * 2 MHz, where K = 0, 1, 2 … 39)
- 3 Channels are fixed for Broadcasting(Advertising) data, whereas other 37 channels are used for communication purposes.
- Data transmission rate can be set to 1 Mbps or 2 Mbps.

Where is the risk ?

Attack Methods



1 Passive Eavesdropping
2 Active Attacks
3 Privacy or Identity Tracking

Bluetooth attacks examples:

Blue-snarf attack -> get personal information

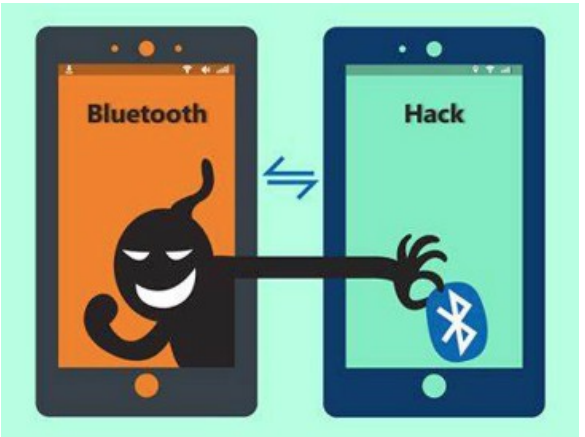
- Hacker's gaining access to people bluetooth enabled device without owner permission.
- allows hackers to send message, make phone calls etc..(hacker to be within 30 ft range)
- To avoid set the phone to non-discoverable mode

Blue-jack attack -> send unwanted messages

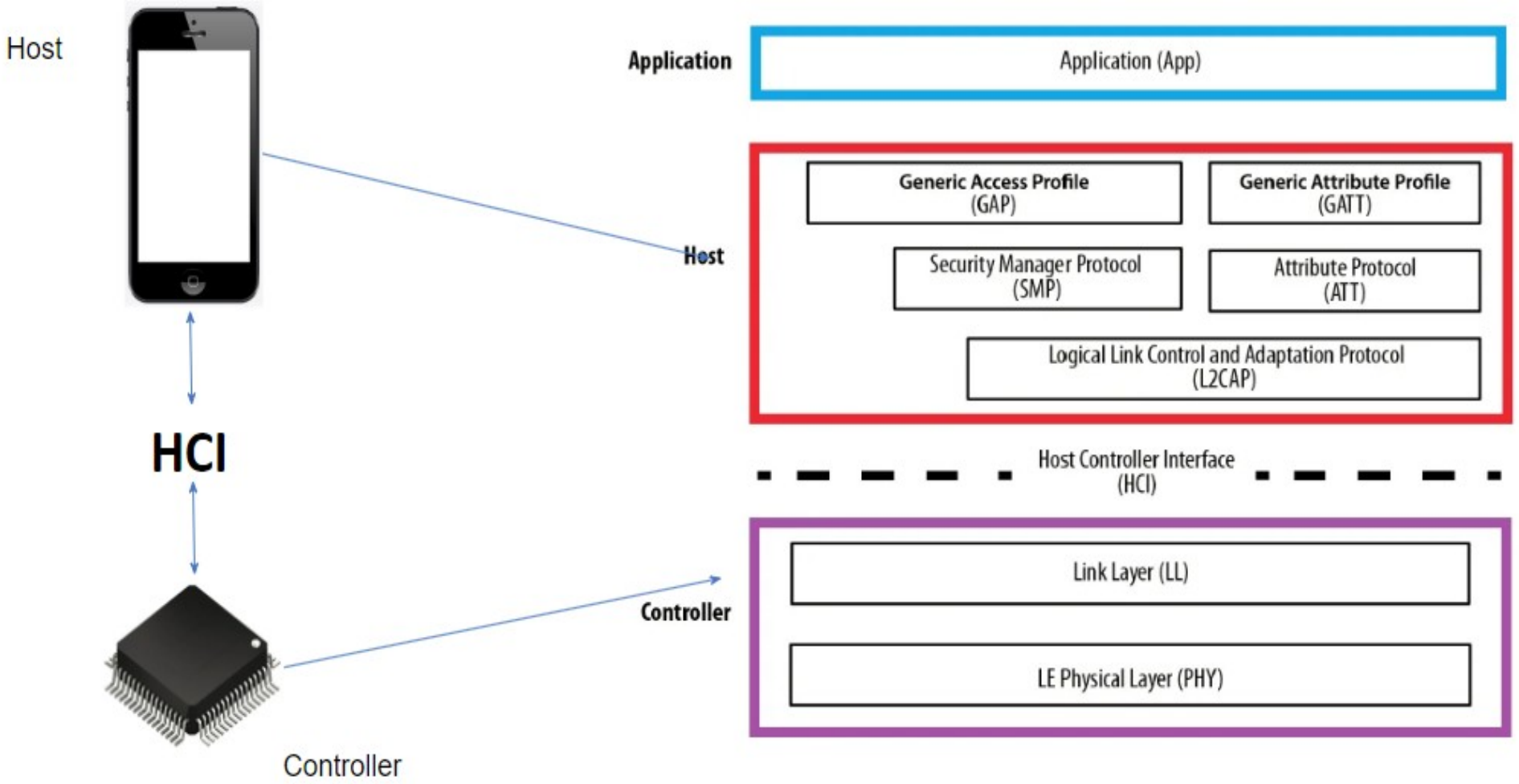
- Funny type message sent to people Bluetooth enabled device without owner permission.

Blue-bug attack -> full access(using AT Command)

- Advanced level of hacking with technology use.
- Hackers gaining access to people bluetooth enabled device mainly to made some harm.



BLE Architecture(BLE Stack)



- **Protocol** is a universally agreed way to communicate between two ble devices
- **Protocol Stack :** is a set of protocols that work together to transmit information from one ble device to another.

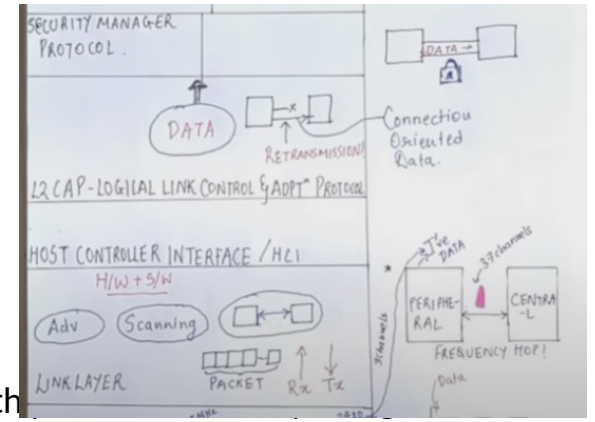
1.physical layer:

- analog communication circuitry.
- concerns with actual transfer of data over air.
- BLE operates 2.4 ghz ISM.
- It performs *modulation/demodulation* of the data into RF signals.it defines physical characteristics of the *bluetooth transceiver.*
- 40 Channels : 3 adv + 37 data channels.

what is advertisement:

ex: 1 ble device is shouting about it presence on those 3 channels.then other device (central) is interested in exchange of data, the data exchanged on that 37 channels using frequency hopping mechanism.

2.Base band link layer:it performs the connection establishment within a piconet



3.Link Layer: combination of H/W +S/W.

- It performs the management of the already established links. it also includes authentication & encryption processes.

3.Physical + Link = controller layer

4.Host layer: pouring data in , pulling the data out.

5.L2CAP: provides data integrity.

- It is the heart of the bluetooth protocol stack.it allows the communication between upper and lower layers of bluetooth packets received from upper layers into the form expected by lower layers. it performs segmentation and multiplexing

6.SMP: Provides pairing and key distribution for secure connection & secure exchange of data.

7.GAP :(GENERIC ACCESS PROFILE) : provides the access to link layer operations.

- defining role of ble device , managing advertisements, connection establishments, security.

8.GATT (Generic attributes): Data exchange in BLE. (DATA LAYER) -> how to bunch ATT attributes.

- devices already gone through advertising process governed by GAP.
- ***Uses att protocol (attributes protocol) for data transfer & how to access data using client-server model. (data stored in attributes which can be accessed by client)***

8.HCI (host controller interface): interoperability between host & controller

BLE Security :

- Security is optional
  - ❖ Authentication & encryption is possible
  - ❖ However, by default, it is not enabled!!!
- Authentication & Authorization
  - ❖ Used to ensure that the connection is established to the correct device
  - ❖ Protect against active Man-in-the-Middle attacks
- Encryption
  - ❖ Used to ensure that no one can read the transmitted data
  - ❖ Protect against passive Man-in-the-Middle attacks
- The security model includes five security features:

  Pairing: the process for creating shared secret key

  Bonding: storing the keys created during pairing so they can be used later

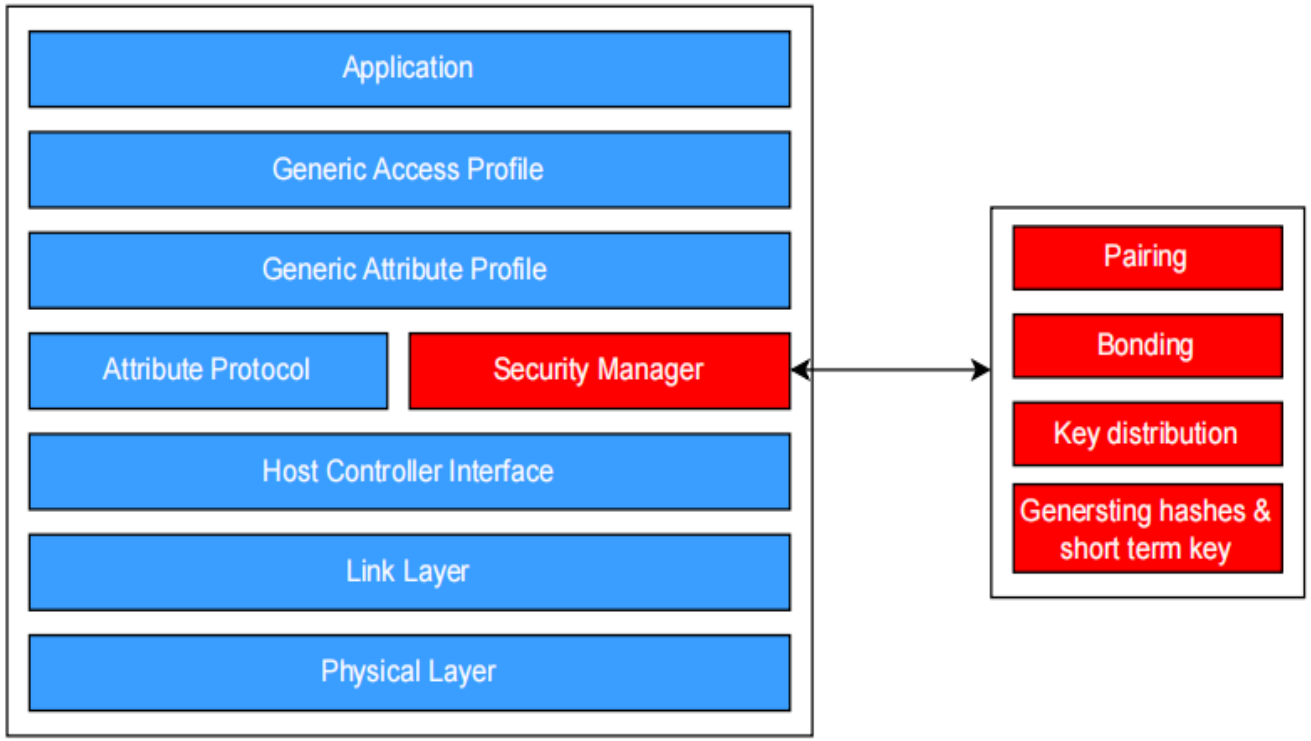
  Device authentication: verification of stored key

  Encryption: data confidentiality

  Message integrity: protection against data alteration

BLE Security - Security Manager (SM)

- Defines pairing, authentication, encryption, key exchange/distribution, …

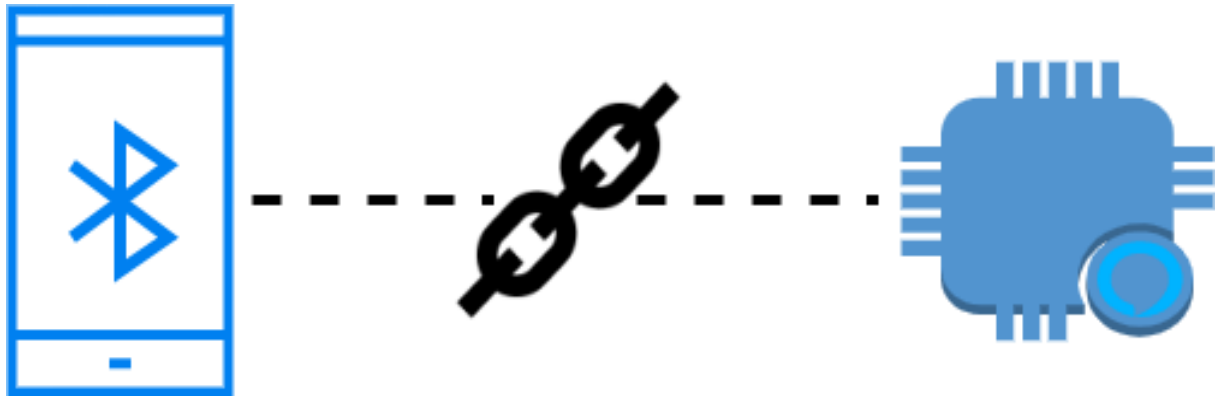


BLE Security - Security Manager (SM)

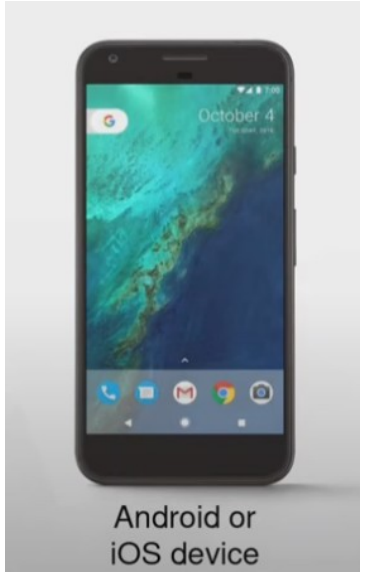
- There are two types of pairing based on BLE version:
  - LE Legacy Pairing (supported in Bluetooth 4.0 and 4.1)
  - LE Secure Connections (introduced in Bluetooth 4.2)

- In version 4.0 and 4.1 of the core specification, BLE functionality uses the secure simple pairing model (now known as LE Legacy), which uses an insecure key exchange algorithm.

- In version 4.2, security is enhanced by the new LE secure connections pairing model. In this model, the numeric comparison is added to the LE Legacy methods and the Elliptical Curve Diffie-Hellman (ECDH) algorithm is introduced for key exchange in this process.



Bluetooth Sniffing Tools:



nRF Sniffer

So ? Is it secure or not ?

- Practice most of the device do not implement BLE layer encryption.
- Mobile application cannot control the pairing.

Recommendation

- Purchase BLE devices from official channels. Before purchasing, search for BLE security information.
- Please turn on the device only when in use and connect the device immediately after it is turned on. Please turn off the device when it is idle.
- Check and update the device firmware regularly.
- Timely rollout of updates to fix BLE product vulnerabilities.


Thank
You!