Bluetooth Security

Mohit Sethi
Ericsson, Finland
Aalto University, Finland

Bluetooth Security - Outline

- Part 1:
  - – Bluetooth standard evolution
  - – Bluetooth stack and protocols
- Part 2:
  - – Pairing and Bonding
  - – Privacy with Private addresses
- Part 3:
  - – Mesh and secure joining

Bluetooth

- Developed by Ericsson in 1994
  - Named after Danish king Harald Blåtand Gormsen
- Standard specified by the Bluetooth SIG (Special Interest Group) together with Nokia, IBM, Intel, Toshiba etc.
- Major releases
  - Bluetooth 2.0 – 2004
  - Bluetooth 4.0 – 2010
  - Bluetooth 5.0 – 2016
  - Bluetooth Mesh profile – 2017

Bluetooth Standard Evolution

- Bluetooth 2.0 and 2.1 :
  - Lower power consumption and faster data transfer (≈ 3Mbit/s)
  - Secure Simple Pairing made pairing simpler and more secure
- Bluetooth 4.0 and 4.2:
  - Bluetooth Low Energy (BLE) aka Bluetooth Smart
  - Health and fitness trackers with longer battery life
  - IPv6 and improved Internet connectivity
  - Beacons and advertisements
  - Privacy enhancements with better protection against device tracking
- Bluetooth 5.0 – 2016
  - Faster and longer range (≈ 240 meters)
- Bluetooth Mesh profile – 2017
  - Mesh networking with 100s of devices
  - Can work with devices that support Bluetooth 4.2 and higher
  - Original Bluetooth from early 2000s defines piconets (1 master + 7 active slave devices). Most deployments were device-to-device!

Bluetooth – Protocol Stack

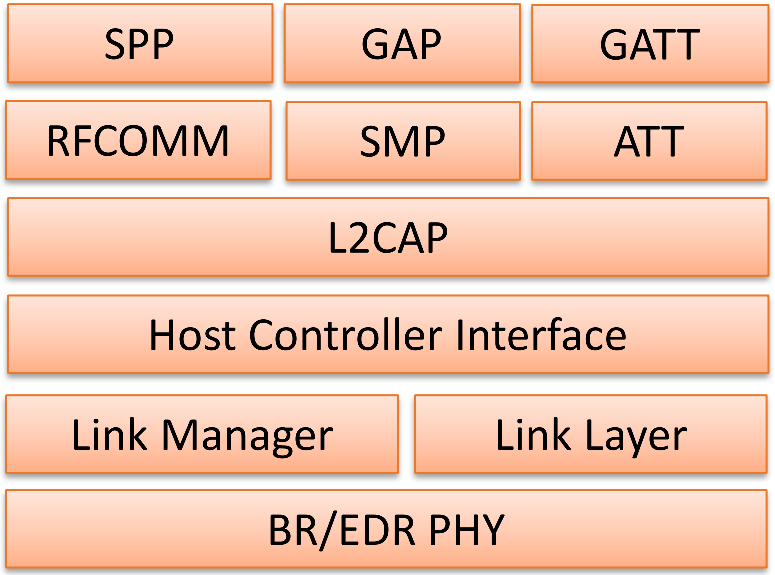
– Bluetooth has two wireless technology systems:

- Basic Rate (BR) : includes optional enhanced data rate (EDR) and Alternate Media Access Control (AMP) extensions
- Low Energy (LE): low power, low cost, low data rates

Bluetooth – Protocol Stack

– Bluetooth has two wireless technology systems:

- Basic Rate (BR) : includes optional enhanced data rate (EDR) and Alternate Media Access Control (AMP) extensions
- Low Energy (LE): low power, low cost, low data rates



SPP | GAP | GATT

RFCOMM | SMP | ATT

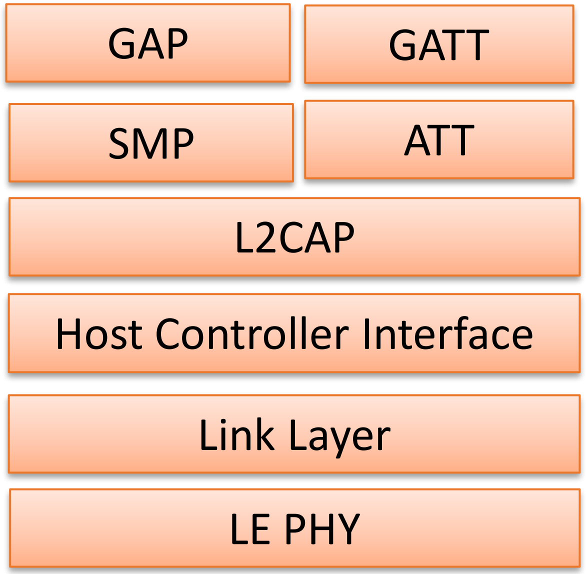
L2CAP

Host Controller Interface

Link Manager | Link Layer

BR/EDR PHY

BR/EDR protocol stack



GAP | GATT

SMP | ATT

L2CAP

Host Controller Interface

Link Layer

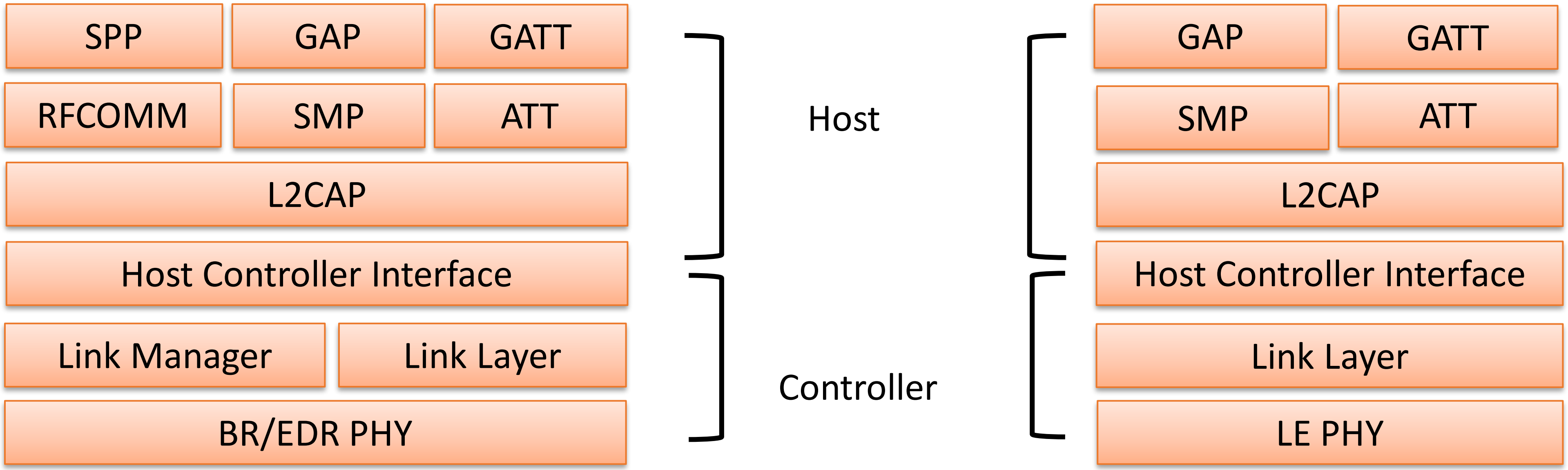
LE PHY

LE protocol stack

Bluetooth – Protocol Stack

– Bluetooth has two wireless technology systems:

- Basic Rate (BR) : includes optional enhanced data rate (EDR) and Alternate Media Access Control (AMP) extensions
- Low Energy (LE): low power, low cost, low data rates



SPP GAP GATT

RFCOMM SMP ATT

L2CAP

Host Controller Interface

Link Manager Link Layer

BR/EDR PHY

Host

Controller

GAP GATT

SMP ATT

L2CAP

Host Controller Interface

Link Layer

LE PHY

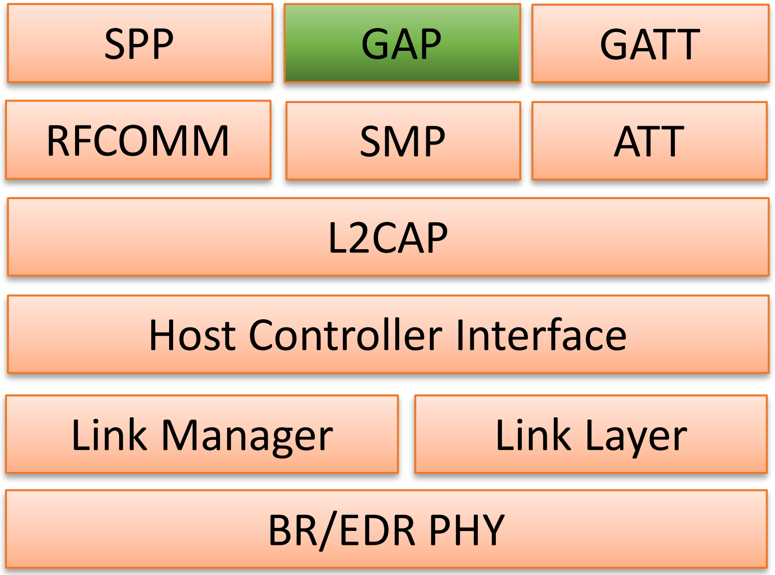
BR/EDR protocol stack

LE protocol stack

Bluetooth – Protocol Stack

– Bluetooth has two wireless technology systems:

- Basic Rate (BR) : includes optional enhanced data rate (EDR) and Alternate Media Access Control (AMP) extensions
- Low Energy (LE): low power, low cost, low data rates



SPP | GAP | GATT

RFCOMM | SMP | ATT

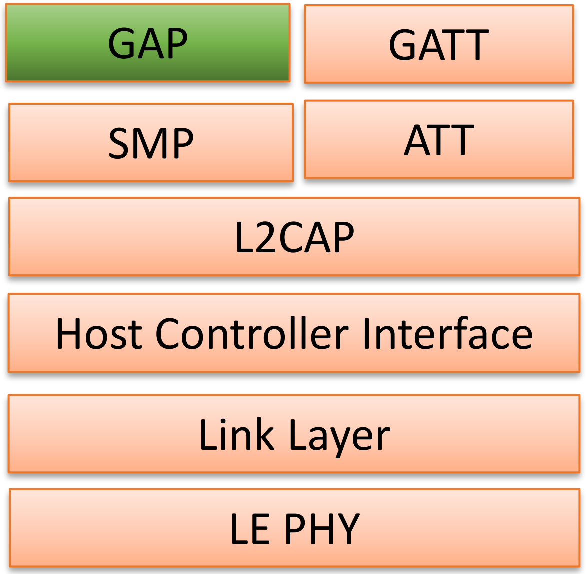
L2CAP

Host Controller Interface

Link Manager | Link Layer

BR/EDR PHY

BR/EDR protocol stack



GAP | GATT

SMP | ATT

L2CAP

Host Controller Interface

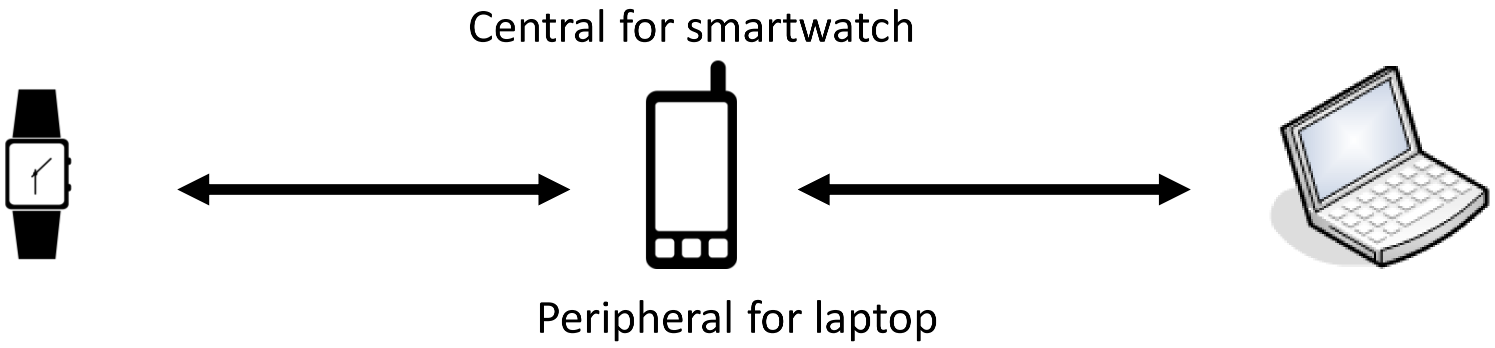
Link Layer

LE PHY

LE protocol stack

Bluetooth – GAP

- Generic Access Profile:
  - Base profile implemented by all Bluetooth devices
  - Defines device discovery, connection establishment, association models, security
- Roles:
  - Single role in BR/EDR – all devices can initiate or accept connections
  - Four roles in LE :
    - Broadcaster: Broadcast device advertises but does not accept connections
    - Observer: Observer listens to advertisements but does not initiate connection
    - Peripheral: Device advertises and accepts a single connection
    - Central: Initiator for all connections and can open multiple connections
  - Simultaneous multiple roles



Central for smartwatch

Peripheral for laptop

Bluetooth – GAP

- GAP defines various modes a device can be in:
  - Discoverability modes
    - Non-discoverable/Discoverable/Limited discoverable/General discoverable
  - Connectability modes
    - Non-connectable
  - Bonding modes
    - Non-bondable/Bondable
  - Synchronizable modes
    - Non-synchronizable/Synchronizable
  - Periodic Advertising mode

Bluetooth – Advertising

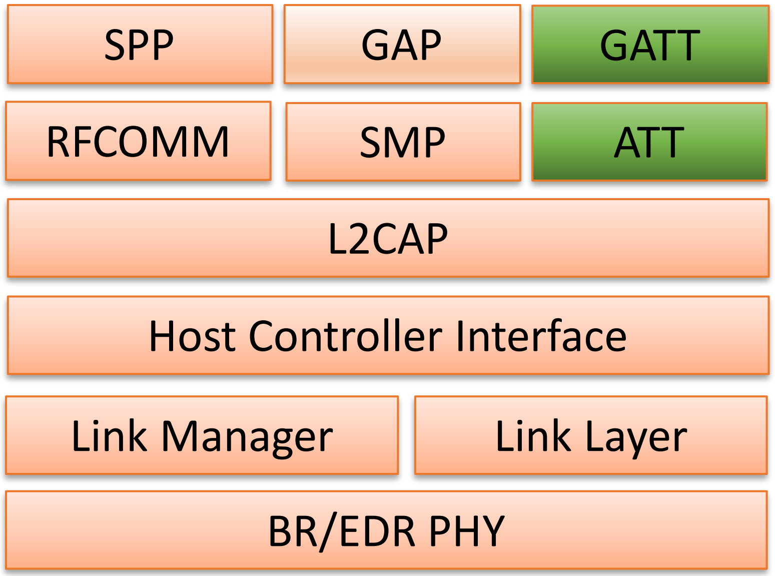
- Advertisements sent by broadcaster or peripheral
- 3 primary channels for advertisements chosen to avoid overlap with WiFi
- Advertisements can be: directed/undirected/connectable/non-connectable/scannable/non-scanable
- 31 bytes of data that includes:
  - Device name
  - Service UUID (Universally Unique Identifier)
- 2 popular standards that build on Bluetooth Advertising
  - Apple iBeacon
  - Google Eddystone
- Used for indoor positioning, asset tracking etc.

Bluetooth – Connections

- Advertisements are unidirectional
- Connections enable bidirectional data transfer
- Several phases before connection establishment:
  - Inquiry and name discovery
  - Link establishment
- In LE: Peripheral -> Slave and Central -> Master
- In BR/EDR: initiating device is master and responding device is slave
  - Role switching is possible: initiating device wants to joining an existing piconet
- Connection request -> data exchange -> connection established
- If no existing link key for authentication and encryption, then pairing is necessary.

Bluetooth – GATT

- Generic Attribute (GATT) Profile
  - How is data formatted and exchanged between a client and server
  - Builds on ATT (Attribute Protocol)



SPP GAP GATT

RFCOMM SMP ATT

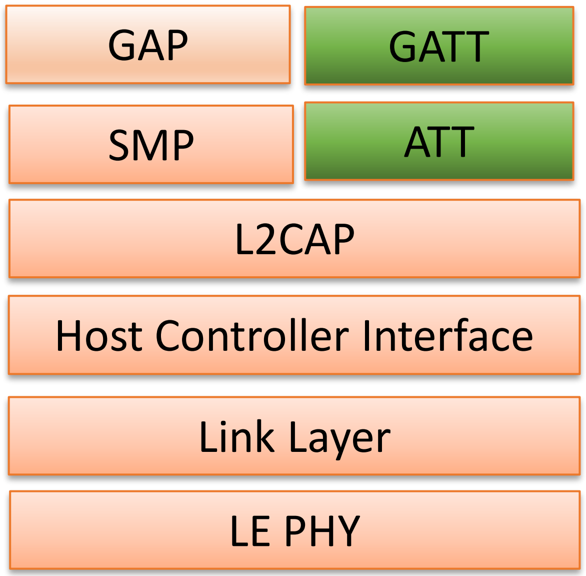
L2CAP

Host Controller Interface

Link Manager Link Layer

BR/EDR PHY

BR/EDR protocol stack



GAP GATT

SMP ATT

L2CAP

Host Controller Interface

Link Layer

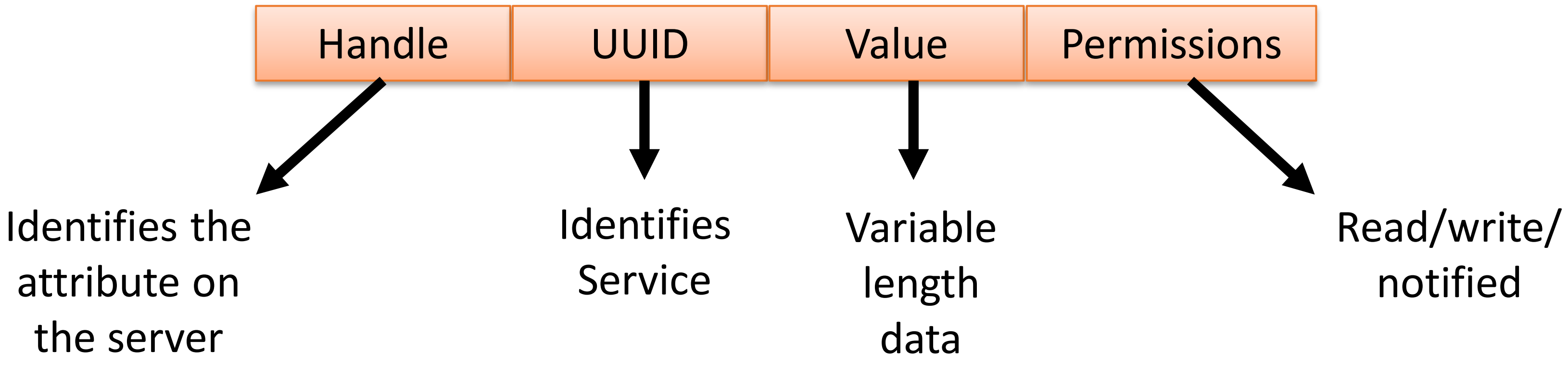
LE PHY

LE protocol stack

Bluetooth – GATT

- Attribute (ATT) protocol:
  - Defines how a server exposes data and clients read/query/commands
  - Data is structured as attributes
  - Client/server role independent of master/slave
  - Devices can be in both client and server role

Attribute Structure



Handle	UUID	Value	Permissions
Identifies the attribute on the server	Identifies Service	Variable length data	Read/write/ notified

Bluetooth – GATT

- A service is composed of attributes
  - Characteristic attributes: contain a value that can be read by the client.
  - Can include optional descriptor attributes that help define value it holds (format/unit)
- A profile is composed of services and defines client/server behavior
- Generic Attribute (GATT) profile:
  - defines how to use ATT for discovery, reading, writing, and obtaining indications
  - reference framework for other GATT-based profiles: SIG defined or custom

Next Video

- Part 2:
  - Pairing and Bonding
  - Privacy with Private addresses