Designing for Success: Leveraging Security Features of Bluetooth for Your IoT Applications

All registered trademarks or trademarks are property of their respective owners. Information described herein is furnished for informational use only, is subject to change without notice, and should not be construed as a guarantee, commitment, condition or offer.
Meet Your Presenters:

Jonathan Kaye  
Product Director

Jennifer Gibbs  
Field Applications Engineer
Today’s Agenda

1. Bluetooth Spec – Background
   - BTv4.0 to 4.2
   - Bluetooth 5
2. Bluetooth Security – SMP
3. Bluetooth Security – Pairing, legacy to LE Secure Connections
5. Q&A
Evolution of the Bluetooth Core Specifications

- 1998: Bluetooth SIG formalized
- 1999: Bluetooth v1.0 released
- 2004: Bluetooth v2.0 + EDR
- 2007: Bluetooth v2.1 + EDR
- 2009: Bluetooth v3.0
- 2010: Bluetooth v4.0 Arrival of BLE
- 2013: Bluetooth v4.1
- 2014: Bluetooth v4.2
- 2016: Bluetooth 5
The two most prevalent implementations of the specification are Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR), which was adopted as version 2.0/2.1, and Bluetooth with low energy (BLE), which was adopted as version 4.0/4.1/4.2.

Each implementation has different use cases and each implementation uses a different chipset to meet essential hardware requirements. Dual-mode chipsets are also available for applications that include both use cases.

### Changing Terminology for Bluetooth

- **a.k.a.**
  - “Bluetooth Classic”
  - “Bluetooth Low Energy”, “BLE”
  - “Dual-Mode Bluetooth”

- **application**
  - Streaming data-rich content (audio, video, etc.)
  - Transmitting small amounts of data at low duty cycles (sensors, remotes, etc.)
  - Ability to connect and interact with both BT and BT Smart peripherals

- **examples**
  - Audio headsets, wireless speakers
  - Sensors, Home automation, remote FOBS
  - Smartphone, Tablet, Laptop
# BTv4.2 – The Focus for Security Improvements

<table>
<thead>
<tr>
<th>ADVANTAGES</th>
<th>FEATURES</th>
<th>END USER EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry-Leading Privacy</td>
<td>LE Privacy 1.2</td>
<td>A Bluetooth Smart location tracker can only be followed by the owner or trusted</td>
</tr>
<tr>
<td>Keeps Bluetooth Smart devices from</td>
<td></td>
<td>group all while consuming less power</td>
</tr>
<tr>
<td>being tracked</td>
<td></td>
<td></td>
</tr>
<tr>
<td>More Power Efficient</td>
<td>LE Secure Connections</td>
<td>A Bluetooth Smart lock or other smart home device provides industry standard</td>
</tr>
<tr>
<td>Introduces refinements that help</td>
<td></td>
<td>security for added user confidence during device pairing</td>
</tr>
<tr>
<td>Bluetooth Smart devices save even</td>
<td></td>
<td></td>
</tr>
<tr>
<td>more energy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Highly Secure</td>
<td>Available early 2015</td>
<td></td>
</tr>
<tr>
<td>Features FIPS-compliant encryption</td>
<td>through the HTTP Proxy Service</td>
<td></td>
</tr>
<tr>
<td>ensuring confidential data stays</td>
<td>(HPS) &amp; RESTful API white papers</td>
<td></td>
</tr>
<tr>
<td>that way</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Information in charts cited from Bluetooth SIG White Paper - “BLUETOOTH® CORE SPECIFICATION 4.2 FREQUENTLY ASKED QUESTIONS”*
Bluetooth 5’s Arrival in Late 2016

- Core specification release just last month
- Always a lag of 6 – 12 months plus before commercially available implementations hit the market, including new phone/tablet models
- No major security updates but focus on 3 major new features

<table>
<thead>
<tr>
<th>ADVANTAGES</th>
<th>FEATURES</th>
<th>END USER EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robust, reliable connections indoors and outdoors</td>
<td>4 x Range</td>
<td>Whole house/building coverage/outdoor e.g. Nordic Semi tests drone connectivity to 750m outdoor range!</td>
</tr>
<tr>
<td>Faster data transfer, reduced TX / RX time</td>
<td>2 x Speed</td>
<td>Lower latency, increased performance &amp; faster data transfer for critical data e.g. swifter FW updates, download of logged sensor data</td>
</tr>
<tr>
<td>More data capacity in Connectionless Services</td>
<td>8 x Increase broadcast message capacity</td>
<td>Beacons &amp; location/tracking services can be improved for greater data &amp; information e.g. enhanced user experiences in facility tours</td>
</tr>
</tbody>
</table>
Bluetooth Low Energy Security and Privacy

• What are we protecting against?

Man-in-the-Middle Attacks, Active Eavesdropping
• Unauthenticated keys

Passive Eavesdropping
• Keys with low entropy or insecure key generation and distribution

Tracking
• Broadcasting Identity Information (E.g. Mac Address)

A → B

C

A → B

Tracking

A

X
Security Manager Protocol (SMP)

- LE Security and Privacy is managed in the Host by the Security Manager Protocol (SMP) over a dedicated L2CAP channel to the Link Layer (LL) in the Controller.

- SMP is responsible for managing the storage and generation of encryption and identity keys as well as generation and resolution of random addresses.
LE Security Modes

**LE Security Mode 1**
1. No Security – No Authentication and No Encryption
2. Unauthenticated pairing w/ encryption
3. Authenticated pairing w/ encryption
4. Authenticated LE Secure Connections pairing w/ encryption

**LE Security Mode 2**
1. Unauthenticated pairing w/ data signing
2. Authenticated pairing w/ data signing
LE Security Modes

Security requirements are set per Service or Service Request or can be set at the Device level

If a mixture of LE Security Mode 1 and LE Security Mode 2 are requested then LE Security Mode 1 will be enforced

Authentication in LE Security Mode 1 is achieved by enabling encryption and the security of the encryption is impacted by the type of pairing performed: Authenticated pairing or Unauthenticated pairing
Security in BLE: Pairing

Phase 1: Pairing Feature Exchange
- Same for BT4.0 through BT5
- Exchange I/O capabilities which determine Authentication method and whether or not Bonding is to occur
- Exchange OOB availability
- Exchange Authentication requirements
- Exchange Key size requirements
- Specify which keys to distribute in Phase 3

Phase 2: Authentication and Encryption
- Different for BT4.0/4.1 and BT4.2/5
- Authentication, using AES-CMAC, method determined in Phase 1
- AES-CMAC 128 is a FIPS approved symmetric key block cipher algorithm that is used to authenticate plaintext data using an AES-128 block cipher
- Encryption key generation using Diffie Hellman, a FIPS approved Public/Private key exchange algorithm

Phase 3: Transport Specific Key Distribution
- Different keys distributed in BT4.0/4.1 and BT4.2/5
- Identity Resolving Key and static address transmitted during this phase
- Only encrypted phase of pairing process
- Bonding is optional and is the storage of key information in non-volatile memory for later use
Phase 1: Pairing Feature Exchange

- Keyboard Only
- Keyboard/Display
- Display Only
- Display Yes/No
- No Input/Output

- Just Works - Unauthenticated
- Passkey Entry - Authenticated
- Numeric Comparison - Authenticated
- Out-of-Band (OOB) – Authentication based on method used for OOB transfer

- I/O Features of both Initiator and Responder determine the Authentication method used

- Authenticated, MITM protection, means eavesdropper cannot insert their own values into the key exchange process
Phase 2: Authentication and Encryption

**LE Legacy, BT4.0/4.1**

- The Temporary Key (TK) is generated using Passkey Entry, OOB, or Just Works pairing methods.
- TK is authenticated in Passkey Entry & OOB (strength of authentication depends on method used for OOB transfer).
- TK is used to generate Short Term Key which will be used to encrypt Phase 3 & subsequent connection.

**LE Secure Connections**

- Elliptic Curve Diffie Hellman Public Key is transmitted & Diffie Hellman Key is generated.
- Numeric Comparison, Passkey Entry, OOB methods are used to Authenticate confirmation values.
- LTK computed from Diffie Hellman Key & authenticated values.
- Just Works uses Numeric Comparison but is unauthenticated with no MITM protection.
Phase 3: Transport Specific Key Distribution

**LE Legacy, BT4.0/4.1**

- Link encrypted using STK (short term key) from Phase 2
- CSRK, IRK, EDIV, RAND, LTK (long term key), and Public or Random Static Address distributed
- Keys added to Trusted Device Database and can be used to build Whitelists

**LE Secure Connections**

- Link encrypted using LTK from Phase 2
- If both devices support Secure Connections and are BR/EDR+LE devices the LTK can be used in cross-transport key generation to derive the BR/EDR link key so pairing does not need to occur on both transports
- CSRK, IRK, Public or Random Static Address are distributed
- Keys added to Trusted Device Database and can be used to build Whitelists
LE Legacy Security Concerns

- TK is used as the key to generate the STK which encrypts the connection
- TK is subject to Passive Eavesdropping because it is either 0 for Just Works or an easily guessed value for Passkey Entry
- LTK is transmitted over-the-air in Phase 3

LE Legacy Pairing has no Passive Eavesdropping protection
LE Secure Connections

Elliptic Curve Diffie Hellman P-256 Public/Private Key Exchange is a FIPS approved Symmetric Key exchange algorithm

One-way Elliptic Curve functions

Used to provide protection against Passive Eavesdropping

AES-CMAC authentication is used during Phase 2 to authenticate values used to derive Long Term Key and protect against MITM attacks

LTK is derived and never sent over the encrypted link
**LE Secure Connections – Elliptic Curve Diffie Hellman**

Bob

- $g, p$ (Agreed upon per spec)
- $SK_b$ (Private, never leaves Bob)

$$g^{SK_b} \mod p = PK_b$$

$$PK_a^{SK_b} \mod p = DHkey$$

Alice

- $g, p$ (Agreed upon per spec)
- $SK_a$ (Private, never leaves Alice)

$$g^{SK_a} \mod p = PK_a$$

$$PK_b^{SK_a} \mod p = DHkey$$

Eve

- Broadcasted Information

**DHkey calculates to the same value on both ends and it is then used to derive the Long Term Key (LTK)**

Eve cannot compute $SK_a$ or $SK_b$ from the data she has, it is a Discrete Logarithmic Problem (One-way Function) due to the Elliptic Curves the mathematics is based upon.
LE Addressing

BLE has 4 MAC address types:

- IEEE Public
- Random Static
- Random Private Resolvable
- Random Private Non-Resolvable

A BLE radio can use any of these address types and can use multiple address types during operation and can change certain types as often as it likes.
LE Privacy involves the use of the Random Resolvable Address type and requires that Key Distribution occurs in Phase 3 of the pairing process where the IRK is transmitted.

Once Key Distribution has occurred then the SMP or LL can use the IRK to resolve the Random Resolvable Address that is transmitted by the BLE device.

Devices supporting the Privacy feature will set a timer equal to Tgap and update/change the Random Resolvable Address upon Tgap expiry while Broadcasting, Scanning, or Connected. Tgap is undefined and can be any time value.
LE Privacy v1.2

As of BTv4.2, LE Privacy v1.2, the SMP can provide a Resolving List to the LL so random addresses can be resolved by the Controller which can save power in the device by allowing filtering of known devices using Resolvable Private Addressing.

LE Privacy v1.1 required that all Random Resolvable Addresses be passed to the Host and SMP directly for resolution.
For More Information...

- Elliptic Curve Diffie-Hellman YouTube Explanation: https://www.youtube.com/watch?v=F3zzNa42-tQ
Q&A / Wrap-Up
BL652 series
Bluetooth® Smart v4.2 + NFC®
Intelligent, Secure, and Ready for the Future of IoT

Features new Nordic nRF52 with ARM Cortex M4F (512K Flash / 64K RAM) for hostless operation

On-board Chip Antenna or IPEX MHF4 connector options available, certified with multiple antenna options

Ultra-small 10 x 14mm footprint

BLE 4.2 + NFC in one integrated solution

Broad certifications and Bluetooth® SIG Qualification

5
Bluetooth® 5 ready hardware!

features innovative, event-driven programming to significantly simplify BLE module integration
Laird Connectivity Solutions is one trusted partner for wireless product development.

**INDUSTRY-LEADING CERTIFIED WIRELESS MODULES**
- Wi-Fi
- Bluetooth
- LoRa
- 802.15.4
- Certified Antenna Options

**COMPREHENSIVE IoT PRODUCT DEVELOPMENT SERVICES**
- Industrial Design
- Antenna & RF Hardware
- Embedded Software
- Mobile App & Cloud Development
- EMC Testing & Certification
- Turn-Key ODM Production