ECEN 5823-001 / -001B

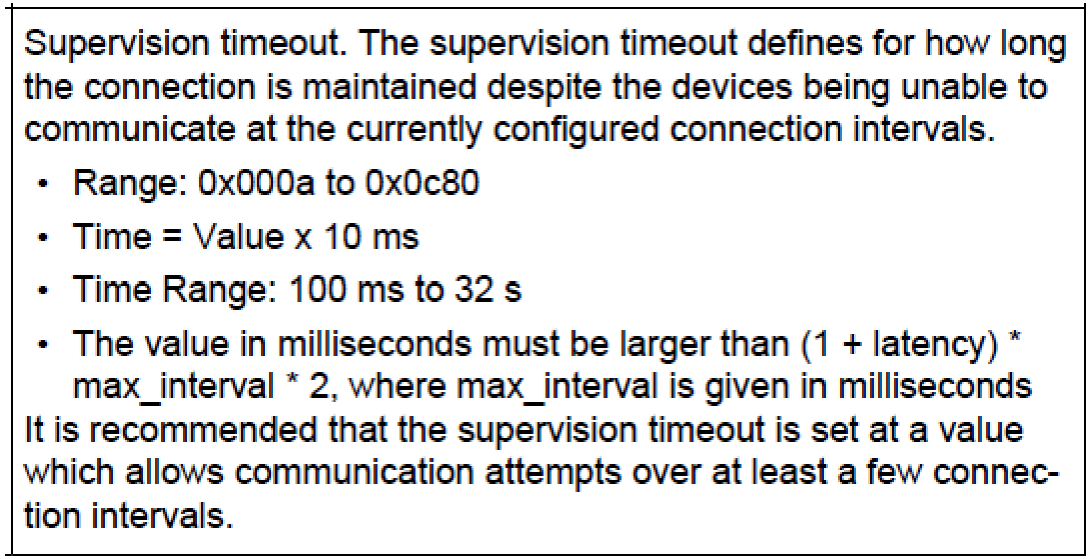
Internet of Things Embedded Firmware

Lecture #19

31 October 2017

Unexpected learning opportunities

- The Blue Gecko API states that the Timeout must be:



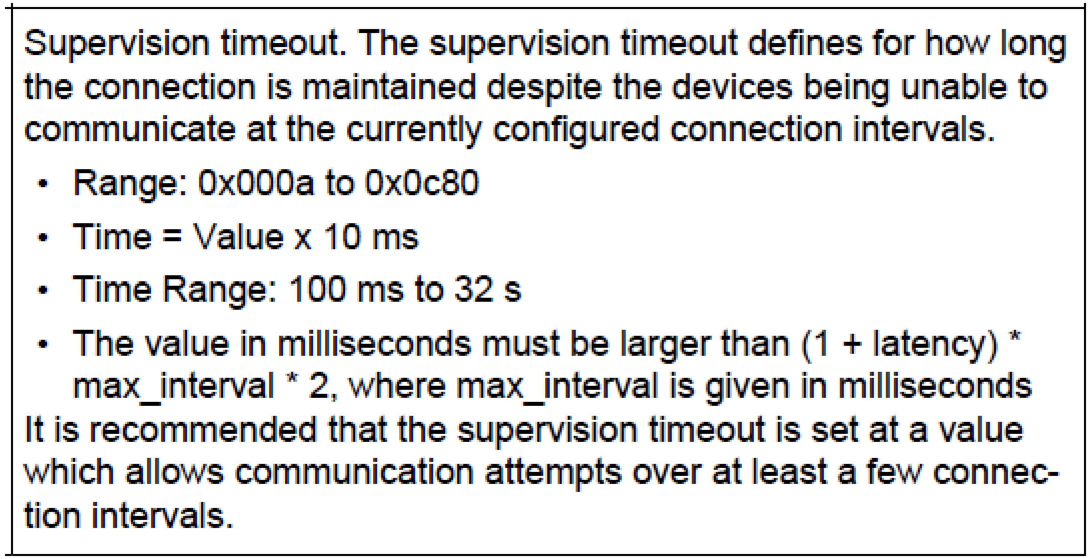
Supervision timeout. The supervision timeout defines for how long the connection is maintained despite the devices being unable to communicate at the currently configured connection intervals.

- Range: 0x000a to 0x0c80
- Time = Value x 10 ms
- Time Range: 100 ms to 32 s
- The value in milliseconds must be larger than (1 + latency) * max_interval * 2, where max_interval is given in milliseconds

It is recommended that the supervision timeout is set at a value which allows communication attempts over at least a few connection intervals.

Engineering is in the implementation

Unexpected learning opportunities



Supervision timeout. The supervision timeout defines for how long the connection is maintained despite the devices being unable to communicate at the currently configured connection intervals.

- Range: 0x000a to 0x0c80
- Time = Value x 10 ms
- Time Range: 100 ms to 32 s
- The value in milliseconds must be larger than (1 + latency) * max_interval * 2, where max_interval is given in milliseconds

It is recommended that the supervision timeout is set at a value which allows communication attempts over at least a few connection intervals.

20. To maximize energy savings, the Bluetooth application should change its advertising, connection interval, and slave interval to what is appropriate to the application.
    a. Set the Advertising min and max to 500mS
    b. Set Connection Interval minimum and maximum to 75mS
    c. Set the Slave latency to enable it to be off the “air” up to 375mS

Agenda

- Class announcements
- Course Project
- Bluetooth Smart
- Bluetooth Mesh

Class Announcements

- No quiz this week
- Course Project Proposal is due this Saturday the 4th at 11:59pm
- BLE assignment Rubric

Reading Assignment

Note: There is no quiz this week, but the material from this reading assignment will be on the final.

1. “Bluetooth Low Energy, The Developer’s Handbook,” by Robin Heydon

   ISBN: 978-0-13-28836-3

   Chapter 10: Attributes

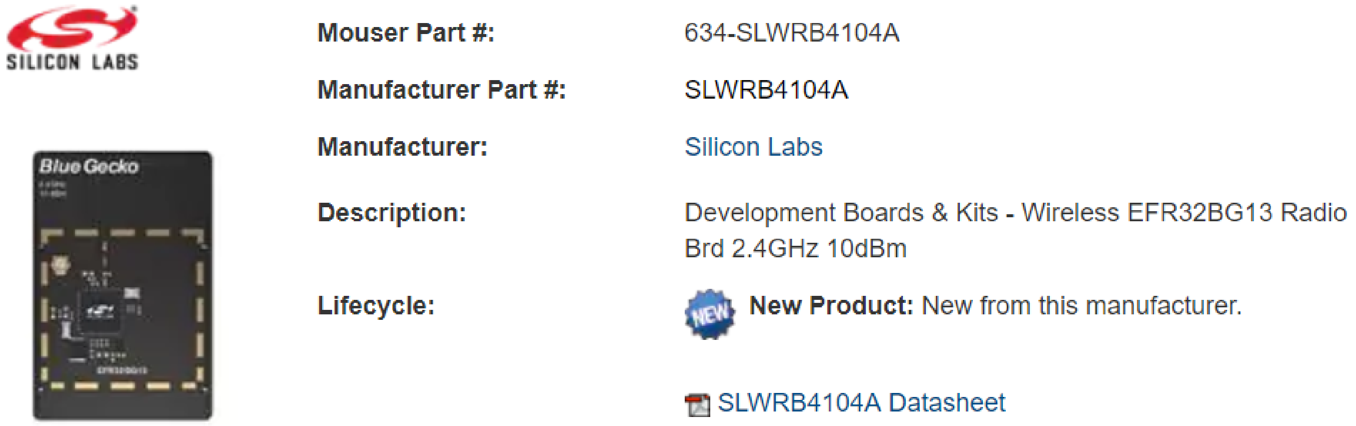
2. “Bluetooth Low Energy, The Developer’s Handbook,” by Robin Heydon

   ISBN: 978-0-13-28836-3

   Chapter 11: Security

Place your sensor request on the following Google Sheet !!!

- https://docs.google.com/a/colorado.edu/spreadsheets/d/1fNUuaJ-69DEbhiX6ZufN6sRnKK9lEzBg-cTpXQGtF5o/edit?usp=sharing
- Orders must be in by this Saturday the 4th at 11:59pm
- If you are planning on a Bluetooth Mesh project, please include the proper Blue Gecko dev kit radio module



Mouser Part #:	634-SLWRB4104A
Manufacturer Part #:	SLWRB4104A
Manufacturer:	Silicon Labs
Description:	Development Boards & Kits - Wireless EFR32BG13 Radio Brd 2.4GHz 10dBm
Lifecycle:	NEW **New Product:** New from this manufacturer.
	SLWRB4104A Datasheet

BLE: Attribute Protocol

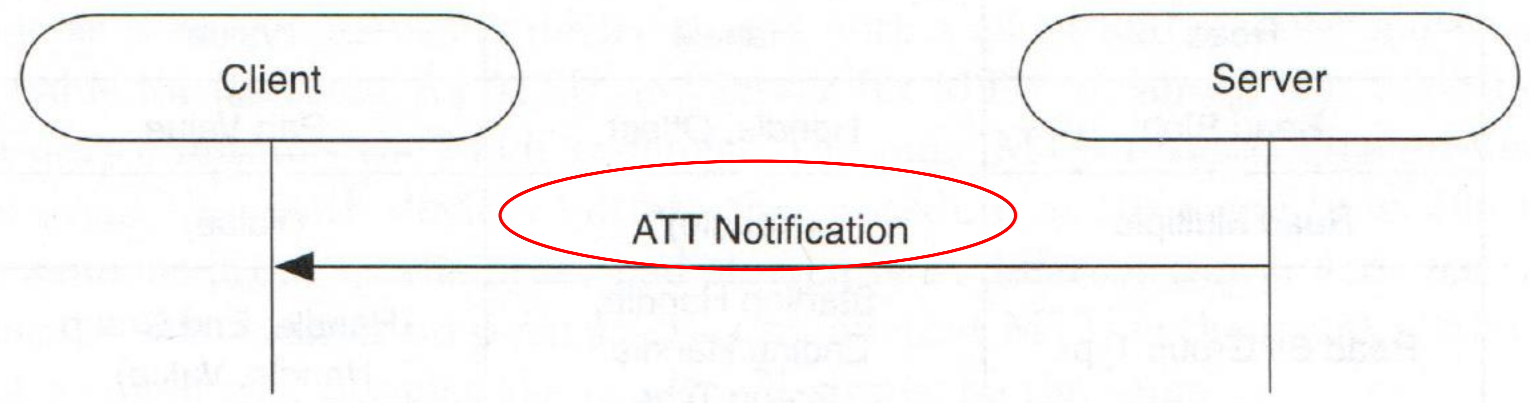
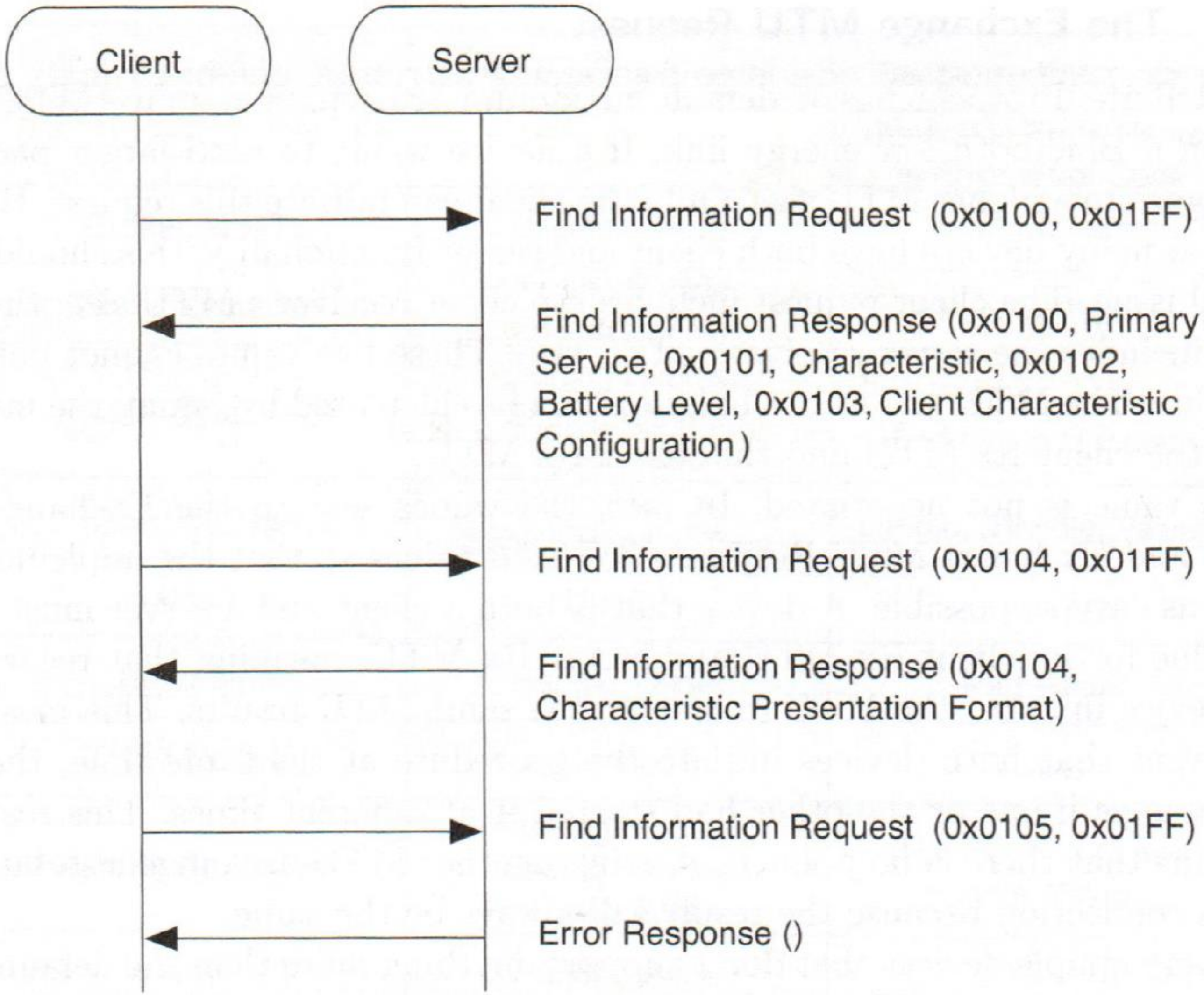


Figure 10–29 An Attribute Protocol notification

- The server can send notification to a client to inform a client that a value of a particular attribute has changed, but does not require a confirmation

BLE: Attribute Protocol

- Find Information Request and Response
  - Find handle and type information for a sequence of attributes
  - The requests includes two handles: a starting handle and an ending handle
  - Typically, the response packet is too short to complete this request, so the client must repeat the operation with incrementing the starting handle to be one more than the last response handle



Client

Server

Find Information Request (0x0100, 0x01FF)

Find Information Response (0x0100, Primary Service, 0x0101, Characteristic, 0x0102, Battery Level, 0x0103, Client Characteristic Configuration)

Find Information Request (0x0104, 0x01FF)

Find Information Response (0x0104, Characteristic Presentation Format)

Find Information Request (0x0105, 0x01FF)

Error Response ()

Figure 10–31 The Find Information Request

Bluetooth Low Energy: The Developer's Handbook
By Robin Heydon

BLE: Attribute Protocol

- Find By Type Value Request
  - Finds all the attributes with a given type and value
  - The request includes a starting and an ending handle
  - Primary use of this request is to find all the primary services
  - Example:
    - A client can send a Find By Type Value Request with the type set to Primary Service and the value set to the UUID of the service
    - The response then includes the handle range of each instance of this primary service located
  - Secondary services are always included from other services, so the Ready By Type Request is used to discover these services

BLE: Attribute Protocol

- Read By Type Request
  - Reads the value of an attribute within a range of handles
  - Used by the client who wants to know the attribute types within a range of handles, and not the handle
  - Each attribute within the handle range that has the requested type is returned
    - The response is a set of attribute handles and their associated values
  - Primarily used to search for included services as well as discovering all the characteristics of a service by using the Characteristic type
  - Example:
    - The client wants to quickly read the battery level of a device, read by type request set to "Battery Level" will respond with the attributes handle and values
    - No need to send a secondary read request using the attribute handle

BLE: Attribute Protocol

- Read Request
  - Simplest Attribute Protocol request
  - Request includes a handle, and the response returns the value of the attribute identified by the handle
  - Only useful after the attribute's handle has been identified
- Read Blob Request
  - Blob comes from the database term meaning Binary Long Object
  - If the value of an attribute is longer than what can be contained within a Read Response, a Read Blob Request is used
  - The Read Blob Request includes the handle as well as a given offset into the attribute's value
  - Example:
    - The Read Blob Request can be used after a Read Request that returned the first 22 octets of the attribute value
    - The Read Blob Request would use the same handle with an offset of 22

BLE: Attribute Protocol

- Read Multiple Request
  - Reads multiple attribute values in a single operation
  - The request includes a set of one more attribute handles
  - The response includes the value of these attribute handles in order they were requested
- Ready By Group Type Request
  - Takes a range of handles that the read will be considered over as well as an attribute type
  - The response will includes the handle of the read attribute and the last attribute for the grouping of attribute
  - Example:
    - If the grouping type is a Primary Service, the response will include the Primary Service attribute handle and the last handle of the last attribute of that grouping
    - This single request would return the entire range of handles for a Primary Service as well as the value of the Primary Service

BLE: Attribute Protocol

- Write Request
  - The request includes a handle and the value written into that attribute
  - The response acknowledges that the value was written into the attribute
- Write Command
  - The command includes the handle of the attribute and the value to be written
  - There is no response
- Signed Write Command
  - Similar to the Write Command except it also includes an authentication signature

BLE: Attribute Protocol

- Prepare Write Request and Execute Write Request
  - Used for two purposes
    - First, provide the ability to write long attribute values
    - Second, allow multiple values to be written in a single-executed atomic operation
  - The values prepared to be written are not written into the attribute until the Execute Write Request is received with the go-ahead to execute the writes
  - The Prepare Write Request includes the handle, offset, and part attribute value in a similar way as that of a Read Blob Request
  - This insures that all parts of the attribute are written at the same time
  - The Prepare Write Response includes the handle, offset, and part attribute value for the client to check and insure that the correct write was received

BLE: Attribute Protocol

- Handle Value Notification
  - Used by the server to send a quick attribute state update to a client
  - The server provides the attribute handle and value
  - The serve can update the client with attribute values or notify the client of changes in a finite state machine
  - The client does not respond to these notifications
- Handle Value Indication
  - Similar to the Handle Value Notification in that it provides the attribute handle and value, but it requires a confirmation receipt from the client
  - Because of the confirmation, indications are considered reliable while notification are not

BLE: Attribute Protocol

- Error Response
  - An Error Response can be sent by a device whenever a request cannot be achieved
  - The Error Response includes all the information about the request that cause the error, the attribute on which the request failed, and why the error was generated
  - Whenever the client receives an error response, it must assume that the error response is for the last request that was sent
    - Thus, and error response is another way to close the request's transaction

BLE: Attribute Protocol

- Possible Error Responses are:
  - Invalid Handle
  - Read Not Permitted
  - Write Not Permitted
  - Invalid PDU
  - Insufficient Authentication
  - Request Not Supported
  - Invalid Offset
  - Insufficient Authorization
  - Prepare Queue Full
  - Attribute Not Found
  - Attribute Not Long
  - Insufficient Encryption Key Size
  - Invalid Attribute Value Length
  - Unlikely Error
  - Insufficient Encryption
  - Unsupported Group Type
  - Insufficient Resources
  - Application Errors

BLE & Security

- Definitions
  - Authentication: Prove that the device is who / what it claims to be
    - Two basic methods:
      - Initial authentication and sharing of a secret
      - Re-authorization using a previously shared secret
    - In BLE, authentication is performed in three different ways
      - At initial pairing, an authentication algorithm is used to authenticate the devices
        - This allows shared secrets to be stored, and the devices are said to be “bonded”

BLE & Security

- Definitions
  - In BLE, authentication is performed in three different ways (continued)
    - Upon reconnecting to a device in which the devices have previously bonded, one of the devices sends a signed command to the other device to authenticate that it knows the shared secret
    - Since the signature is created using the shared secret exchanged during bonding, it cannot be falsified
    - The signed command process must include some revolving algorithm to prevent replay attacks.
  - When reconnecting to a device that has previously been bonded, either device can initiate encryption
    - From the moment onwards, all packets will incorporate Message Integrity Check (MIC) value that authenticate the sender of the message

BLE & Security

- Definitions
  - Authorization: Assigning of permission to something
    - Documentation that provides authorization
    - Authorization that is actioned directly
  - Authentication ≠ Authorization

  - Integrity: Internal consistency and lack of data corruption
    - Cyclic Redundancy Checks (CRC) are used to protect against bit changes, but they are typically too week to be considered a security measure
      - Valid CRD ≠ Integrity

BLE & Security

- Confidentiality: the intent to keep something secret
  - In BLE, confidentiality refers to that even if a third-party receives a message, they cannot decode it
  - In BLE, confidentiality is provide via encryption
- Privacy: The ability to prevent others from recognizing you by the device you are carrying and not allowing them to track your movement throughout space

BLE & Security

- A key in BLE is shorthand for shared secret
- There are five types of keys in BLE
  - Temporary Key: A temporary key used during the pairing process that is determined by the pairing algorithm
    - "Just Works" is a mode designed to enable pairing of devices with limited user interface
      - No authentication is being performed
      - It is open to the man-in-the-middle attack
    - "Passkey Entry" is a mode used when the user interface on both devices allow the display or entry of a number value, 0 – 999999
      - With only 1 in 1,000,000 of a chance of a man-in-the-middle attack, this method can generate an authenticated key

BLE & Security

- Temporary Key: A temporary key used during the pairing process that is determined by the pairing algorithm (continued)
  - "Out of Band" is a mode both devices have information that has been acquired by using another technology than Bluetooth

- Short-Term Key: Is a key used for encrypting a connection the very first time two devices pair
  - Utilizes three pieces of information to generate the STK:
    - The Temporary Key
    - Srand
    - Mrand

BLE & Security

- Long-Term Key: The key distributed once the initial pairing procedure has encrypted the connection
  - Upon reconnection to a previously paired and bonded device, the LTK is used to encrypt the link
- Identity Resolving Key: Give a device that knows a peer device the ability to resolve (work out) a peer device's identity
  - IRK enables a device to randomly change its address and become "private"
  - IRK and Authentication are typically combined to insure that the correct device is at the "random address"

BLE & Security

- Connection Signature Resolving Key (CSRK): Provides the receiving device the ability to resolve a signature and therefore authenticate the sender of a message
  - The CSRK is distributed over an encrypted link
  - But, the signed messages do not

BLE & Security

- Pairing involves the following:
  - Exchange of pairing information
  - Authentication of the link
  - Key distribution (becoming “bonded”)

  - Exchange of information
    - First, the device determines the input and output capabilities
      - Depending on the I/O capabilities, the Temporary Key mode will be defined
      - The first secured message is the pairing request that will be returned

BLE & Security

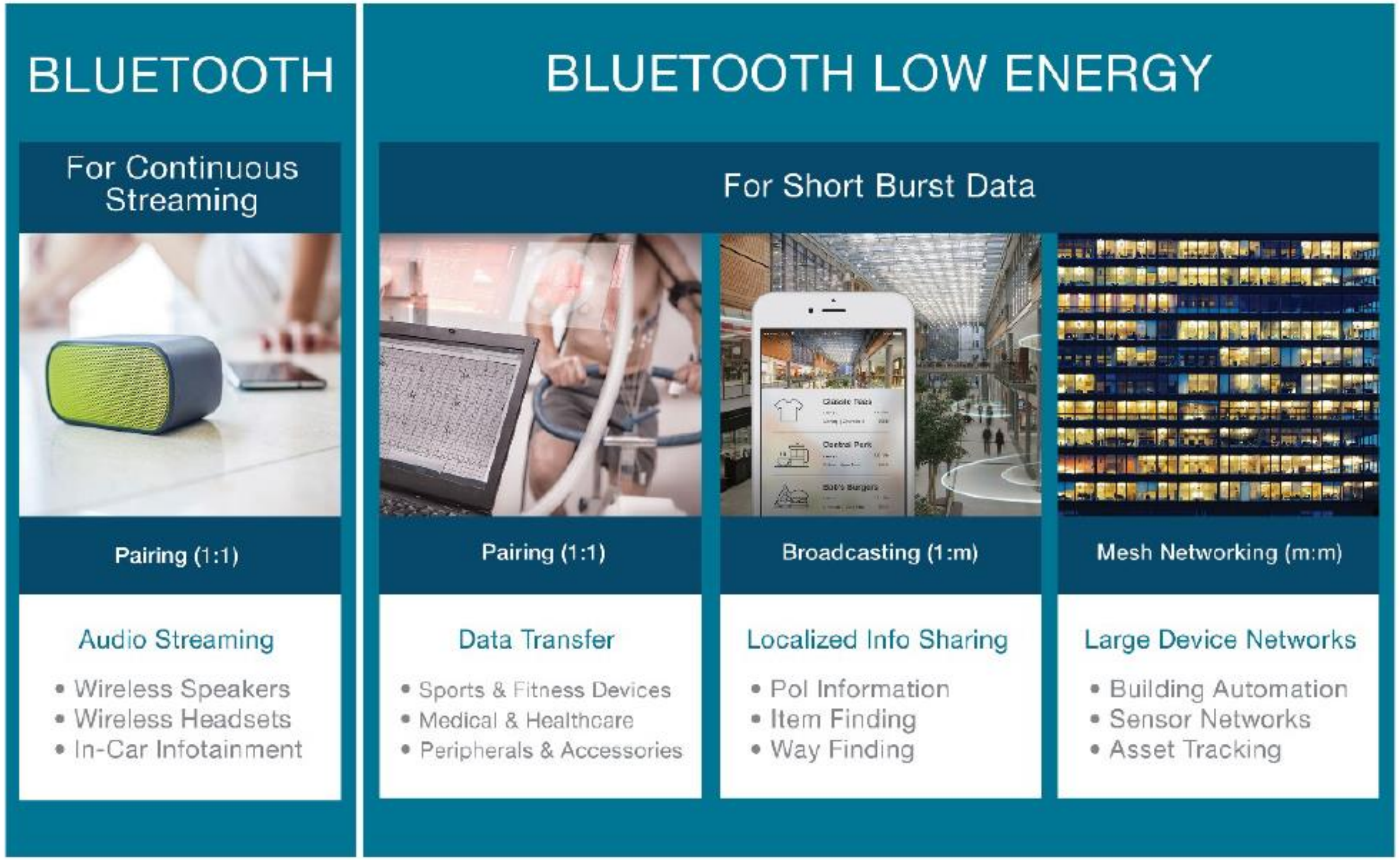
- After resolving the Temporary Key mode
  - The first secured message is the pairing request that will be returned
  - This message will include:
    - What the authentication requirements are, if any, such as whether bonding is enabled and whether man-in-the-middle protection is required
    - List of keys that are being requested
    - The Temporary Key can be generated
  - Once the Temporary Key is generated, the Short-Term Key can be generated to enable the passing of the Long-Term Key, Integrity Resolving Key, and the Connection Signature Resolving Key

https://www.youtube.com/watch?v=5EKoEcSnXP0

Course Project – 1st Bonus Opportunity

- Implementing a Bluetooth Mesh network
- Opportunity is worth 3% towards your final grade!
- Requirements to get the extra credit:
  - Course project demo must receiving a 90% or better
  - Demonstrating an application that utilizes Bluetooth Mesh unique features over Bluetooth Classic and BLE
  - Demonstrating Bluetooth Mesh competence

Bluetooth Mesh



BLUETOOTH

For Continuous Streaming

Pairing (1:1)

Audio Streaming

- Wireless Speakers
- Wireless Headsets
- In-Car Infotainment

BLUETOOTH LOW ENERGY

For Short Burst Data

Pairing (1:1)

Data Transfer

- Sports & Fitness Devices
- Medical & Healthcare
- Peripherals & Accessories

Broadcasting (1:m)

Localized Info Sharing

- PoI Information
- Item Finding
- Way Finding

Mesh Networking (m:m)

Large Device Networks

- Building Automation
- Sensor Networks
- Asset Tracking

Development of Bluetooth standard from Bluetooth BR/EDR (left) to LE and Bluetooth mesh (right)

Silicon Labs’ Bluetooth Mesh: Wireless Technology for the World of IoT

https://www.youtube.com/watch?v=0n1x-wxESaM

Course Project idea

- How can we potentially resolve the out of synch speakers other than positioning them in the room?
- Would Bluetooth Mesh to broadcast simultaneous music to 2 Bluetooth Mesh speakers?

Blue Gecko
SILICON LABS