

ECEN 5823-001 / -001B

Internet of Things Embedded Firmware

Lecture #23

14 November 2017

Agenda

- Class announcements
- Course Project Update #1 assignment
- Bonus opportunity #3 – Persistent Data
- Quiz 8 review
- Bluetooth Mesh

Class Announcements

- Quiz # is due at 11:59pm this Sunday, November 26th, at 11:59pm
- Course Project Update #1 is due at 11:59pm this Saturday the 18th
- Bonus #3, Persistent Data, is due by 11:59pm this Saturday the 18th
 - Since it is a bonus, it must be done during a convenient time for the instructing team and do not expect to get a time at 11:59 on the 18th to demo your OTA bonus assignment
 - This will not be used as an excuse to request an extension
- Any questions regarding the Course Project?
- Any questions regarding Bluetooth Mesh?

Course Project Update #1 assignment

ECEN 5823 Project Update #1 Assignment Fall 2017

Objective: To update the status and provide additional information on the Course Project in ECEN 4593, Fall 2017.

Note: You can use your course project proposal as a base for this project update.

Project Proposal Due Date: Saturday, November 18th, at 11:59pm via D2L drop box

Team proposals: (Include and Provide update to the below items)

1. Describe what problem this project addresses
2. How does this project alleviate or solve the problem?
3. Functional block diagram of the team project
4. Summary of each individual project and how it plays a role in solving the problem
5. Project team members
6. **Team project validation plan**

What comprises a verification plan?

- What each line item should entail?

- What is being verified
- Definition of passing
- Date test performed
- Who completed the test
- Measured result
- Did it pass

| To be verified | Definition of passing | Date test performed | Tested by | Measured result | Passed? |
|--|---|---------------------|-----------|-----------------|---------|
| Digital Vdd does not drop below minimum system specification | Minimum voltage during 3uA to 4mA step at minimum battery voltage (2.4v) above 2.0v | | | | |
| Digital Vdd does not go above system specification | Maximum voltage during 4mA to 3uA step at maximum battery voltage (3.2v) below 3.6v | | | | |

What comprises a verification plan?

- What are the line items that need to be included?
 - Each BLE or Mesh Service or Client profile / model
 - Secure OTA update
 - Persistent Memory functionality
 - LCD driver
 - Any other drivers
 - Include BLE or Mesh security features
 - Bluetooth Mesh node software (Proxy, relay, friend, low power)
 - Complete scheduler
 - Etc.

Persistent Data

- Took about 5 hours to implement
 - 4 hours to figure out how to convert a floating point number into an 8-bit unsigned integer array
 - 1 hour to implement
- How to access a floating point number as an 8-bit unsigned array?
 - Use a union structure
 - **Structures** are used to represent a record. A **union** is a special data type available in **C** that allows storing different data types in the same memory location. You can define a **union** with many members, but only one member can contain a value at any given time. [GeeksforGeeks](#)

Persistent Data

- How to use a C union structure?

```
union {  
    float float_variable;  
    uint8 temp_data_array[data_length];  
} u;  
u.float_variable = temp_set_pt;
```

- Now, you can also access the floating point value via &temp_data_array

Persistent Data

- How to use a C union structure?

```
union {  
    float float_variable;  
    uint8 temp_data_array[data_length];  
} u;
```

Place 8-bit unsigned int array into temp_data_array

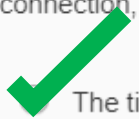
- Now, you can also access the floating point value via &u.float_variable

Course Project – 3rd Bonus Opportunity

- Implementing Persistent Data
- Opportunity is worth **1% towards your final grade!**
- You will need to demonstrate persistent data by changing a value, removing power from your development board, applying power back to the board, and demonstrating different functionality based on the persistent data stored without down loading additional firmware
- Requirements to get the extra credit:
 - Must demo to one of the three instructing team members by Saturday, November 18th at 11:59pm
 - By being a bonus, you must demo during convenient instructing team availability and not expect availability at 11:58pm on November 18th
 - For distant students, the demo should be arranged over video chat, skype, etc.

Quiz 8 review

If two devices are advertising for a connection with identical advertising intervals, and their advertising overlaps each other so that the combined interference prevented either one from finding a connection, what mechanism is used minimize the chance of these two devices interfering with each other on the next advertising event?



The time interval between packets has both a fixed and random delay.

- ☐ Each device will randomly increase or decrease their transmit power enabling one device to potential over power the other device during the next advertising event.
- ☐ Each advertiser will randomly skip 0-10 advertising events to prevent a possible overlap
- ☐ Devices when configured are set with a priority which will be used by the the devices to determine who will have access to the next advertising event

Quiz 8 review

UUIDs uniquely identify Services and Characteristics on a Bluetooth Server. The full UUID is 128 bits in length. How many bytes is the short hand UUID?

☐ 3 bytes

☒ 2 bytes

☐ 1 byte

☐ 4 bytes

Quiz 8 review

Why are connections not allowed by Bluetooth Smart Beacons?

- ☐ Beacons are assets that must be secured, and preventing connections insures their security
- ☒ Once a connection is established, the Beacon would stop participating in advertising events
- ☐ Not entering a connection conserves energy for the Bluetooth Smart Beacon
- ☐ The Beacon has a reduced BLE stack to save cost and energy that prevents it from entering a connection

Quiz 8 review

The BLE master coordinates the medium access between the master and the slave by providing what of the following information. Please select all that apply.

- ☒ Provides the slave the frequency hopping number
- ☐ Sets the slave TX power
- ☒ Determines the instants in which the slave is required to listen
- ☒ Map of which frequency channels that will not be used

Quiz 8 review

What can terminate a connection event? (select all that apply)

- ☒ Corruption of the access address field of the packet sent by either device
- ☐ An indication packet is sent to the master from the slave
- ☐ A response packet with the More Data (MD) bit set
- ☒ Reception of two consecutive packets with bit error by either the master or the slave

Quiz 8 review

What are the possible means of agreeing on a Short Term Key during the bonding process between two BLE devices? (select all that apply)



☒ Out of Band Communications



☒ Passkey Entry



☒ Just Works Method



☐ Transferring an Identity Resolving Key (IRK)

Quiz 8 review

Which BLE key is used to generate the 128-bit key employed for Link Layer encryption and authentication while bonded?

☐ CSRK

☒ LTK

☐ IRK


☐ STK

Quiz 8 review

Which pair modes require Man In The Middle Protection?

- ☐ Just Works with Pairing with Bonding Enabled
- ☐ Just Works Pairing without Bonding
- ☒ Authenticated Pairing with Bonded Enabled
- ☒ Authenticated Pairing
- ☐ Pairing Disabled

Quiz 8 review

To initiate a Bluetooth Server's OTA service, the Bluetooth client writes into the OTA service characteristic using a Bluetooth **(write request)**  (two word answer).

Bluetooth Mesh - Provisioning

- Unprovisioned devices are devices which are not yet part of any Bluetooth mesh network are
- Unprovisioned devices advertise their presence and can be added to the mesh to become nodes of the network by **provisioning**
- The Provisioner such as the mobile device provides the unprovisioned node:
 - Network Key
 - the current IV Index
 - A unicast address for each element in the unprovisioned node

Course Project – 3rd Bonus Opportunity

- Implementing Persistent Data
- Opportunity is worth **1% towards your final grade!**
- You will need to demonstrate persistent data by changing a value, removing power from your development board, applying power back to the board, and demonstrating different functionality based on the persistent data stored without down loading additional firmware
- Requirements to get the extra credit:
 - Must demo to one of the three instructing team members by Saturday, November 18th at 11:59pm
 - By being a bonus, you must demo during convenient instructing team availability and not expect availability at 11:58pm on November 18th
 - For distant students, the demo should be arranged over video chat, skype, etc.

Bluetooth Mesh - Provisioning

- During provisioning network resources are managed and allocated to nodes by a Provisioner
- The Provisioner also allocates node addresses making sure there will be no duplicates of unicast addresses
- Device keys are known only to the device itself and the Provisioner and the device keys are used only during configuration
- The use of multiple Provisioners is allowed but the specifics of cached data sharing etc. need to be defined in the Implementation

Bluetooth Mesh - Device Authentication using OOB

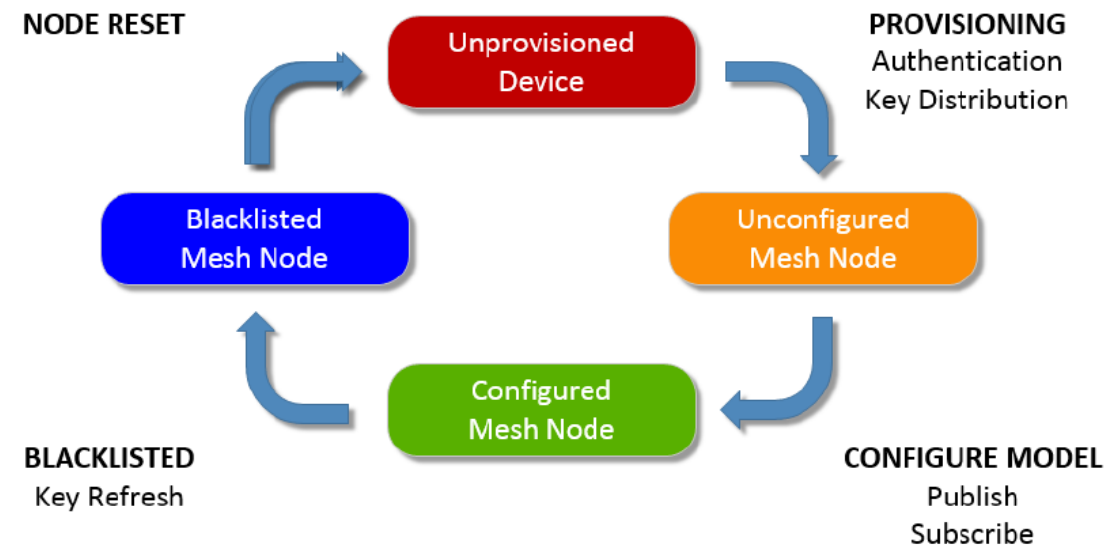
- For secure authentication during provisioning information must be passed between devices without using the actual Bluetooth RF channels, Out-of-Band (OOB) authentication

| Method | Description |
|-------------|---|
| Input | Provisioner outputs a value – user inputs the value into the device |
| Output | Device outputs a value – user inputs the value into the provisioner |
| Out-of-band | Device communicates the value by non-Bluetooth means such as NFC |

Protection against MITM is required!

Bluetooth Mesh - Lifecycle

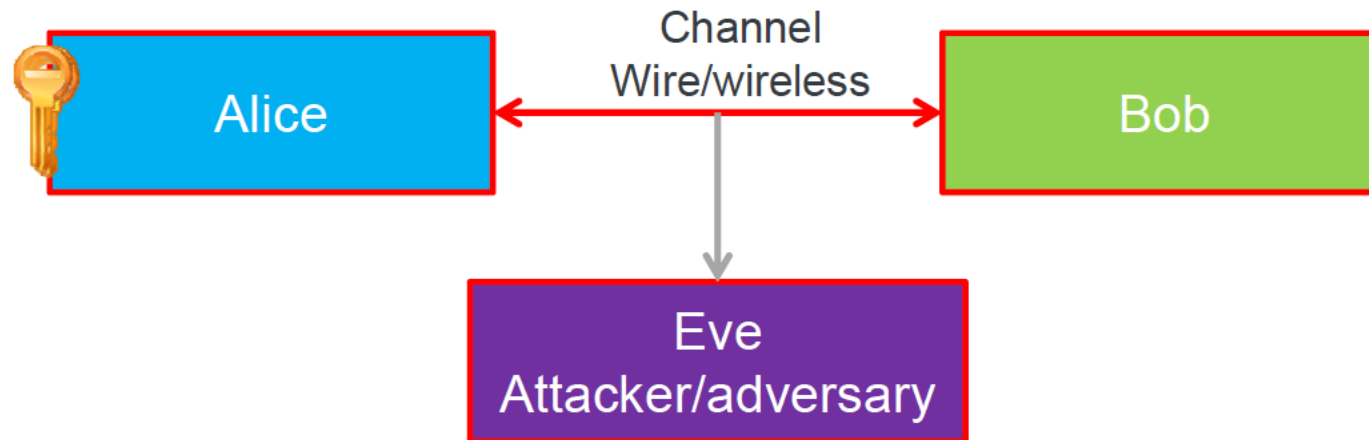
- First the Provisioner must detect an unprovisioned device and establish a provisioning bearer
- Then the Provisioner and the device use the Elliptic Curve Diffie-Hellman (ECDH) anonymous key agreement protocol to establish a shared secret



Bluetooth mesh device lifecycle

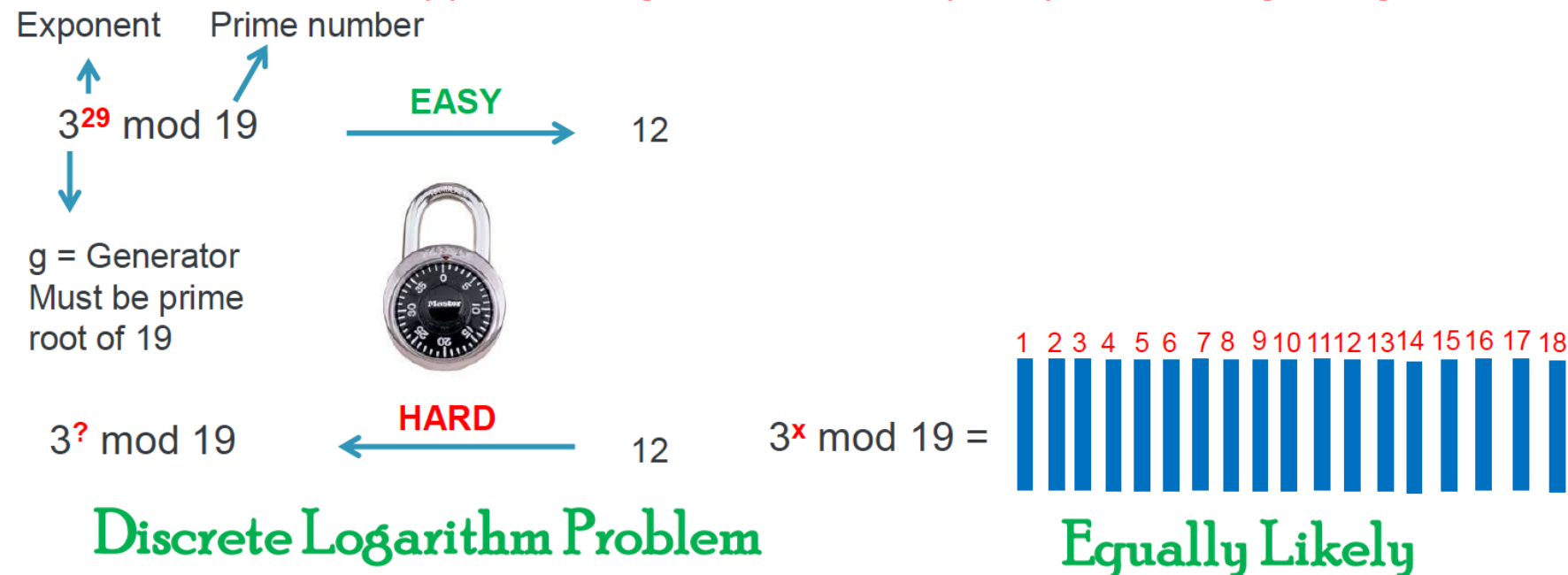
Public Key Cryptography

- Two parties would like to share a secret shared random number (known as a key) in order to transfer data between them
- How could two parties who have never met agree on a secret shared key, without letting Eve who is always listening also obtain a copy?

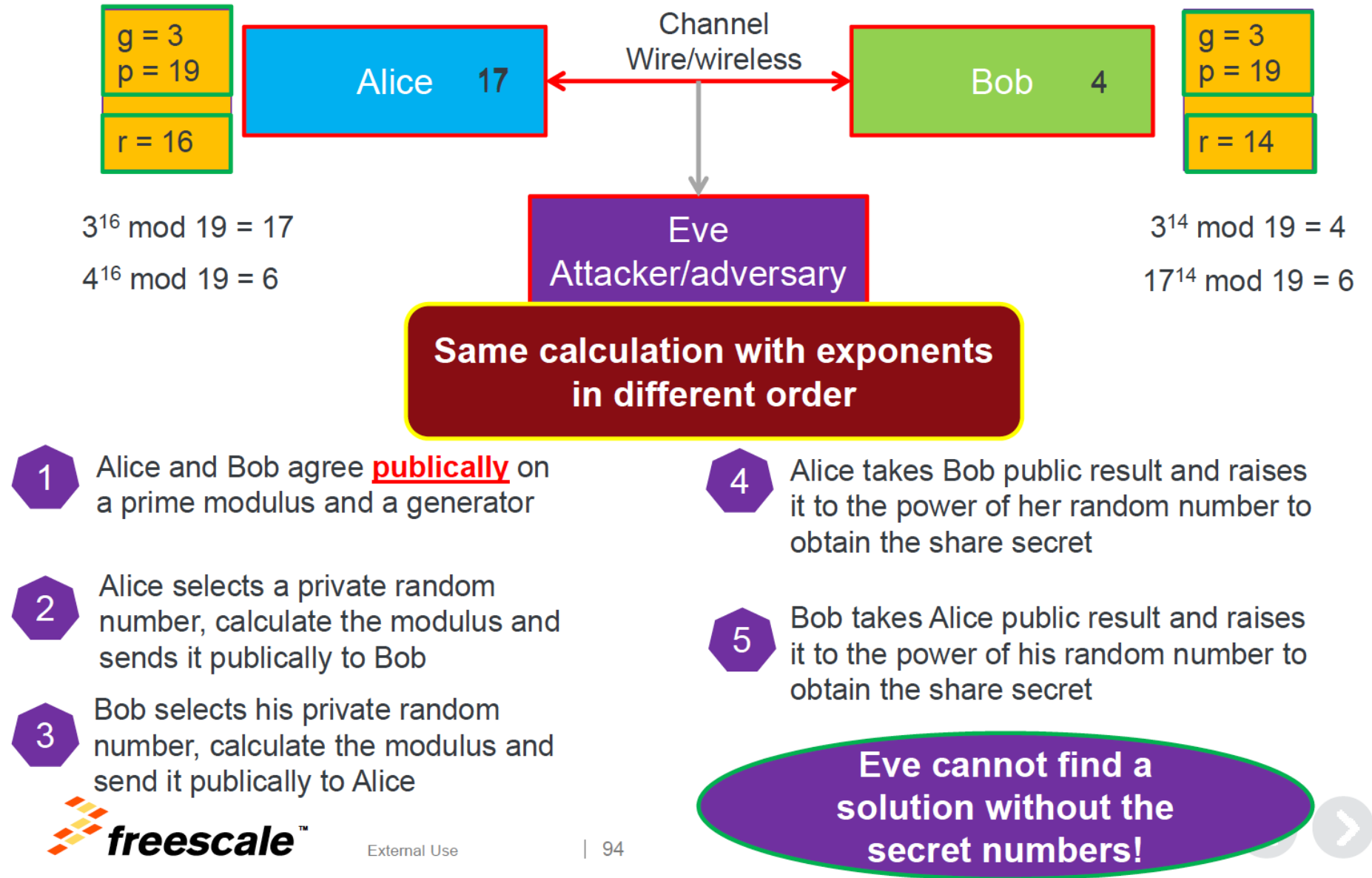


One-Way Function

- In 1976 Whitfield Diffie and Martin E. Hellman advised an amazing trick called the one-way function
 - Numeric procedure that its easy to generate in one direction but hard to reverse
 - Modular arithmetic ($x \bmod p$), known as clock arithmetic
 - The strength of the one-way function is the time needed to reverse it (brute force attack)
- This is not an encryption algorithm, only key exchange algorithm



Diffie-Hellman Key Exchange Algorithm



External Use

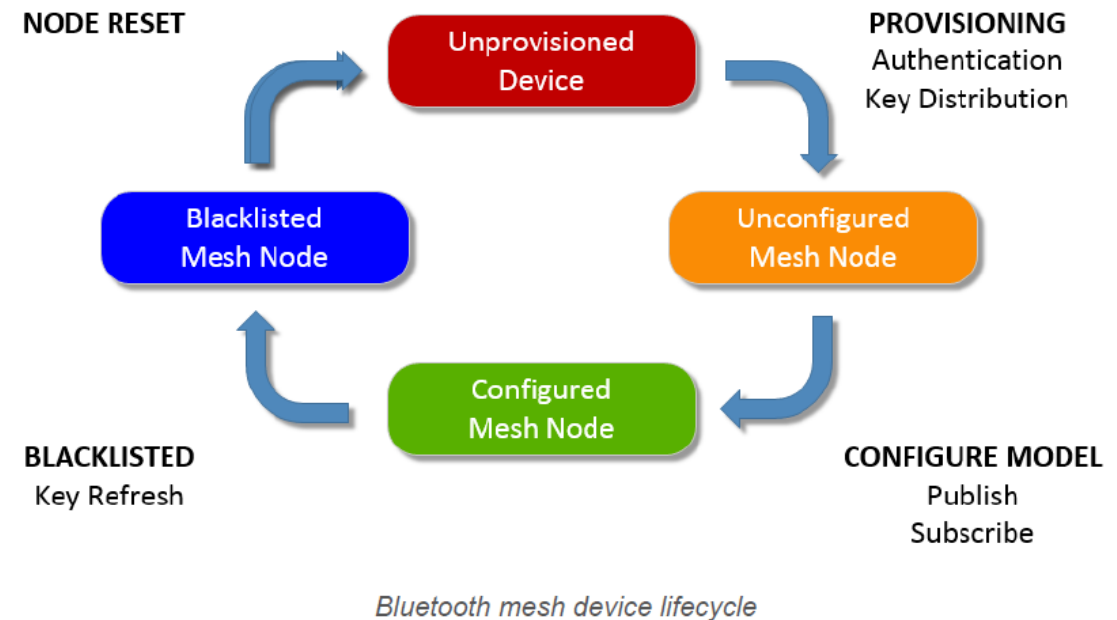
| 94





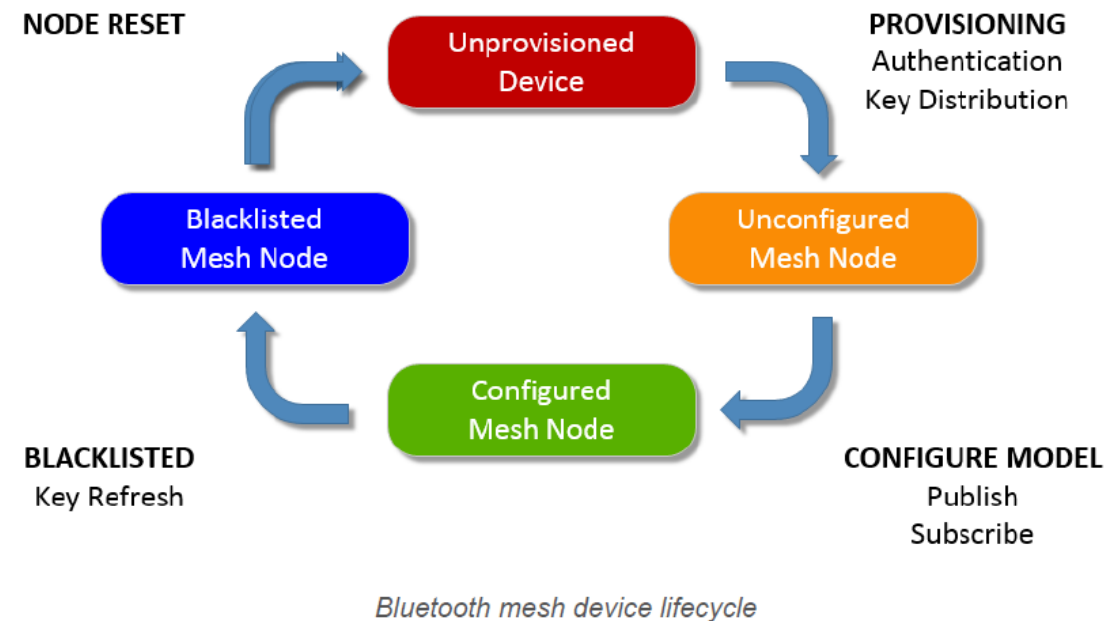
Bluetooth Mesh - Lifecycle

- First the Provisioner must detect an unprovisioned device and establish a provisioning bearer
- Then the Provisioner and the device use the Elliptic Curve Diffie-Hellman (ECDH) anonymous key agreement protocol to establish a shared secret
- After this the device needs to be authenticated using Out-of-Band (OOB) information
- Once authentication has succeeded both the Provisioner and the device together will generate a session key based on the shared secret
- The session key is then used to encrypt and authenticate provisioning data



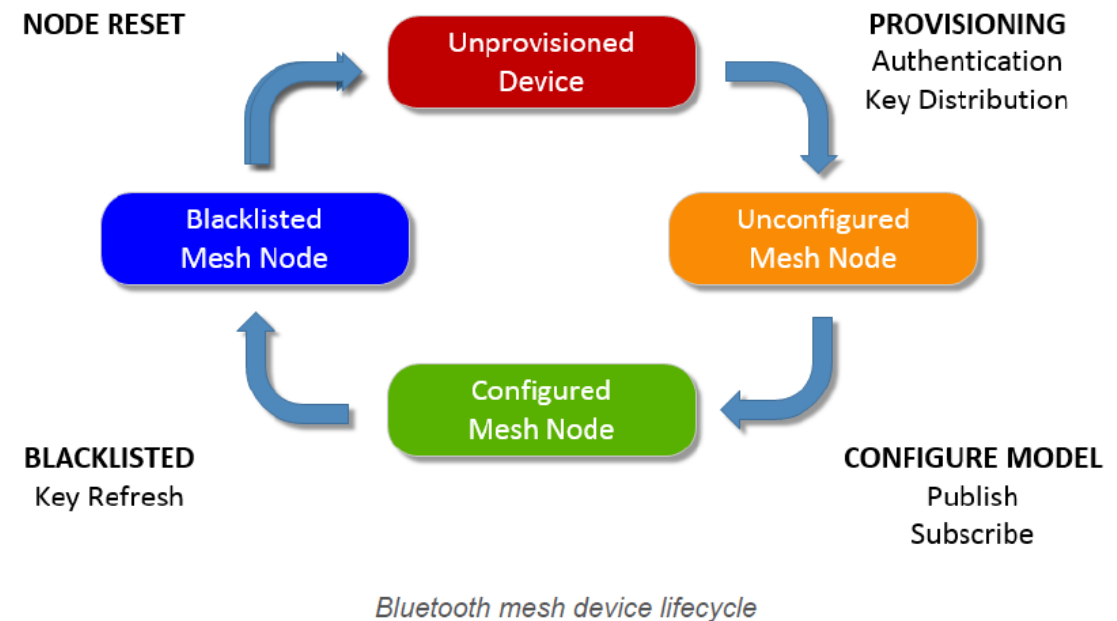
Bluetooth Mesh - Lifecycle

- All devices have a configuration block which includes information such as Company ID, Product ID and Model Information
- The Provisioner needs to read the data contained in the configuration block after which the Provisioner can proceed with the configuration according to the capabilities and Models present on the device
- These keys also need to be bound to the appropriate Network Keys
- Finally, the Provisioner needs to configure how the node publishes information and which information it needs to subscribe to



Bluetooth Mesh - Lifecycle

- If a node is removed from the mesh the keys of all remaining nodes need to be changed to prevent the possibility of a “trash-can attack”
- Nodes which may have been compromised can be blacklisted to prevent their use in the mesh
- Network Keys, Application Keys and all confidential data derived from them can be refreshed using a Key Refresh procedure



Bluetooth Mesh: States

- States are values representing conditions of node elements
 - When an element is exposing a state (value) representing the condition of the element that element is called a Server and implements the Server Model
 - When accessing a state of an node element the accessing node is called a Client, which implements the Client Model
- There are three different methods for controlling element states
 - A state-changing message which is sent to a Server
 - An asynchronous event from the scheduler
 - A local event such as pressing a button

Bluetooth Mesh: Scenes

- Bluetooth Mesh stores states of elements as a Scene
 - A Scene register is a 17-element, zero-based, indexed array of 16-bit values
 - The “handle” of the state is the index into the scene array to state storage containers in which the associated state information is stored