ECEN 5823-001 / -001B

Internet of Things Embedded Firmware

Lecture #15

17 October 2017

Be Boulder.

University of Colorado Boulder

Scheduling your interrupt handlers

- Must use the Gecko's Bluetooth sleep routine to insure that the Bluetooth radio receives control of the Blue Gecko when required
  - `evt = gecko_wait_event();`
- Will switch from using your block and unblock sleep modes to the Gecko's routines
  - `SLEEP_SleepBlockBegin(Timer0_Em);`
  - `SLEEP_SleepBlockEnd(Timer0_Em);`
- The Gecko's Energy Mode enumerations follow the following:
  - sleepEMx where x= the energy mode that is the highest energy mode that this peripheral cannot enter
- Sleep_SleepBlockBegin(sleepEM3) will prevent the Blue Gecko from enter EM3

Scheduling your interrupt handlers

- The Interrupt Service routines should be extremely small and quick
  - The goal is to record what must be done, and then schedule it
- The Blue Gecko through its gecko_wait_event() and the switch statement in the while(1) loop will control when the Service routine is actually handled

Scheduling your interrupt handlers

- Example ISR

```
void LETIMER0_IRQHandler(void){
unsigned int int_flag;

CORE_ATOMIC_IRQ_DISABLE();
int_flag = LETIMER0->IF;
LETIMER0->IFC = int_flag;
if (((int_flag & LETIMER_IFC_UF) != 0) & (si7021_enabled))
external_event_status |= Letimer0_Ext_Evt_Uf;
CORE_ATOMIC_IRQ_ENABLE();

gecko_external_signal(external_event_status);
}
```

Scheduling your interrupt handlers

- To support the external event in the main while(1) loop, there must be a case for the external event
  - `case gecko_evt_system_external_signal_id:`
- Inside this case statement, you will need to determine what caused this case statement to be executed
  - `evt->data.evt_system_external_signal.extsignals`
- Inside this case statement, if statements should be used to determine what service routine to execute instead of a switch statement since more than one interrupt could have occurred since this case statement was last executed

Scheduling your interrupt handlers

- Example of external event if statement

```
if (((evt->data.evt_system_external_signal.extsignals) &
Letimer0_Ext_Evt_Uf) != 0) {
        tempC = get_temp();
        post_temp(tempC);
        temp_ext_evt |= Letimer0_Ext_Evt_Uf;}
if (((evt->data.evt_system_external_signal.extsignals) &
Letimer0_Ext_Evt_Comp1) != 0) {
temp_ext_evt |= Letimer0_Ext_Evt_Comp1;}
```

Scheduling your interrupt handlers

- Before you leave the external event switch statement, you must clear the external event global variable so that it will not be re-executed due to a previous interrupt

```
    CORE_ATOMIC_IRQ_DISABLE();
    external_event_status &= ~temp_ext_evt;
    CORE_ATOMIC_IRQ_ENABLE();
  break;
```

Agenda

- Scheduling your interrupt handlers
- Class announcements
- Quiz 7 review
- Bluetooth Smart

Class Announcements

- No quiz this week
- BLE Health Temperature Service assignment is due at 11:59pm on Sunday, October 29th, 2017
- Mid-term will be held in class on Tuesday, 24th, at 6:30pm in class
  - For on campus students, you must be in class for the exam
  - For distant learners, the mid-term will be due by 11:59pm on Thursday, October 26th, 2017
- There will be no homework assignment or quiz the week of October 16th

Mid-Term

- Tuesday, 24th, at 6:30pm in class
  - For on campus students, you must be in class for the exam
  - For distant learners, the mid-term will be due by 11:59pm on Thursday, October 26th, 2017
- Will be administered by D2L
  - 75 minute time limit for the Mid-term
  - 5 minutes time limit for the bonus section
  - 1 attempt
- Open book, but not open people, not google
- Individual Effort, CU Honor Code

Mid-Term

- Material covered will include:
  - All the readings from the first day of class
  - All the lectures through Thursday, October 19th, 2017
  - All assignments
- Questions:
  - 33 questions that will represent 100% of the mid-term
    - Question pool will be over 100 questions
  - 10 bonus questions each worth 1 point
    - Comprised of a random selection from the first 7 week quiz questions (roughly 150 questions in the question library)

Quiz 7 review

The transmission of packets though advertising channels take place in intervals of time called connection events.

- ○ True
- ○ False

Quiz 7 review

The initiator coordinates the medium access by providing information on the Time Division Multiple Access (TDMA) scheme and provides the slave with the frequency hopping algorithm during which transmission?

- Connection request
- Advertising event
- Connection event

Quiz 7 review

During a connection event, frequency hops could occur if the More Data bit is set signaling that the sender has ore data to transmit.

- ○ True
- ○ False

Quiz 7 review

Every connection event starts with a transmission of a package by the master.

- ○ True
- ○ False

Quiz 7 review

The time between the start of two consecutive connection events is specified by what parameter?

- connInterval
- connEvent
- SlaveLatency

Quiz 7 review

List the sequence in pairing two BLE devices

- Announce their input/output capabilities
- Each end-point can distribute to the other end-point three keys: the 128-bit Long-Term Key (LTK); the Connection Security Resolving Key (CSRK), the Identity Resolving Key (IRK),
- Short Term Key is obtained by both devices
- Agree upon a Temporary Key

Quiz 7 review

For an application where somewhat a real-time response is required, less than 500ms, which settings would you select? (select all that apply)

- [ ] Low connInterval
- [ ] Low SlaveLatency
- [ ] High connInterval
- [ ] High SlaveLatency

Quiz 7 review

The maximum number of slaves that a BLE master can connect to is 7.

- ○ True
- ○ False

3.3. Maximum Piconet Size

We next investigate the maximum piconet size, *i.e.*, the maximum number of slaves that a master can handle. In BLE, each connection between a master and a slave is identified by a 32-bit access address. Beyond this fact, the Bluetooth 4.0 specification does not impose further limits on the number of slaves that can be connected to a master. However, there exist practical limits on that number, depending on the type of communication between master and slave, on the *connInterval* parameter setting and the BER that can be assumed. The maximum piconet size is independent of the *connSlaveLatency* parameter, because the inactive connection events due to slave latency cannot be used for connections with other slaves.

Quiz 7 review

During the initial pairing of devices, when the shared secrets are stored, the devices are said to be _____ (single word answer).

Quiz 7 review

When two BLE devices are reconnecting, either device can initiate encryption. Each and every data packet that is transmitted from then will incorporate the following?

- CRC
- Packet size
- MIC
- Header

Bluetooth low energy devices connected in a link can pass sensitive data by setting up a secure encrypted link. The process is similar to but not identical to *Bluetooth* BR/EDR Secure Simple Pairing. One difference is that in *Bluetooth* low energy the confidential payload includes a Message Identification Code (MIC) that is encrypted with the data. In *Bluetooth* BR/EDR only the data is encrypted. Also in Bluetooth low energy the secure link is more vulnerable to passive eavesdropping, however because of the short transmission periods this vulnerability is considered a low risk. The similarity to BR/EDR occurs with "shared secret key", a fundamental building block of modern wireless network security.

http://www.fte.com/webhelp/bpa600/Content/Documentation/WhitePapers/BTLE/BluetoothSmartSecurity.htm

Quiz 7 review

Which algorithms are used to protect against the man-in-the-middle attack during BLE pairing to obtain the Temporary Key?

- [ ] Just Works
- [ ] Passkey Entry
- [ ] Out of Band
- [ ] Randomization

Quiz 7 review

Order the sequence of a successful pairing of two BLE devices.

- Pairing Response
- Key distribution
- Authentication
- Bonding
- Determines its input and output capabilities

Quiz 7 review

Select the Bluetooth Smart authentication method based on the following:

device 1: Keyboard only

device 2: Keyboard only

- ○ Just Works
- ○ Passkey Entry

	Initiator				
Responder	**DisplayOnly**	**Display YesNo**	**Keyboard Only**	**NoInputNo Output**	**Keyboard Display**
DisplayOnly	Just Works Unauthenti-cated	Just Works Unauthenti-cated	Passkey Entry: responder displays, initiator inputs Authenti-cated	Just Works Unauthenti-cated	Passkey Entry: responder displays, initiator inputs Authenti-cated
Display YesNo	Just Works Unauthenti-cated	Just Works Unauthenti-cated	Passkey Entry: responder displays, initiator inputs Authenti-cated	Just Works Unauthenti-cated	Passkey Entry: responder displays, initiator inputs Authenti-cated
Keyboard Only	Passkey Entry: initiator displays, responder inputs Authenti-cated	Passkey Entry: initiator displays, responder inputs Authenti-cated	Passkey Entry: initiator and responder inputs Authenti-cated	Just Works Unauthenti-cated	Passkey Entry: initiator displays, responder inputs Authenti-cated
NoInput-NoOutput	Just Works Unauthenti-cated	Just Works Unauthenti-cated	Just Works Unauthenti-cated	Just Works Unauthenti-cated	Just Works Unauthenti-cated
Keyboard-Display	Passkey Entry: initiator displays, responder inputs Authenti-cated	Passkey Entry: initiator displays, responder inputs Authenti-cated	Passkey Entry: responder displays, initiator inputs Authenti-cated	Just Works Unauthenti-cated	Passkey Entry: initiator displays, responder inputs Authenti-cated

Table 2.5: Mapping of IO Capabilities to STK Generation Method

Quiz 7 review

Select the Bluetooth Smart authentication method based on the following:

device 1: Keyboard and Display

device 2: Display only

- ○ Just Works
- ○ Passkey Entry

BLE: Peripheral (Connection)

- For practical purposes in terms of saving energy, it does not make sense to set the slave latency to have a maximum time between connections greater than 1s or fewer than 300mS
  - Below 300mS, the power used to repeatedly synchronize is higher than it would be to wait long
  - Above 1s, the power used by window widening does not save any significant amount of power, and the user experience is enhanced with a smaller slave latency

BLE: Peripheral (Stay Connected or Disconnect)

- Two main questions to answer:
  - Can the central device reconnect back to the peripheral in a reasonable latency if the peripheral starts to advertise?
  - If the peripheral does stay connected, can the peripheral inquire the connection latency being used or ask for a connection latency to enable an acceptable battery life?
- The peripheral can obtain from the central device the connection latency that it will honor to the peripheral when reestablishing a connection if the peripheral exposes the Scan Parameters Service
  - The central device that connects to this peripheral will discover the scan parameter service and provide to the peripheral its latency


kasa
SMART LIGHTING
veho
0:07 / 1:55
powered by veho
CC
HD

Bluetooth-Classic: Profiles

- High level description to differentiate between Bluetooth-Classic and BLE profiles
- Why are there Bluetooth-Classic profiles?
  - They provide an interoperability between the master and slave
  - For example, enabling a Bluetooth-Classic headset to work with any Bluetooth-Classic or dual-mode phone
- How does the Bluetooth-Classic profile enable interoperability?
  - Clearly defines and states the responsibility of the master and its commands to the slave within a given profile
  - Clearly defines and states the responsibility of the slave and how it responses to the master within a given profile

Bluetooth-Classic: Profiles

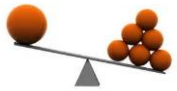
- Are there any drawbacks to the Bluetooth-Classic Profiles?
  - It does not allow, or at least easily, the change of roles or use cases
  - For example:
    - Bluetooth-Classic headsets support the Headset Profile (HSP) which enables interoperability with all Bluetooth-Classic phones
    - As an audio engineer, you discover a new way to send data to the headset that would increase audio fidelity
    - You develop the code on your phone, but since the definition of how the master (phone) operates with the slave (headset) is defined, your new and improved communications scheme will not work on any of the older HSP headsets
    - You will need to convince the headset manufacturers to support a new profile to enable your improved product to market

BLE: Profiles

- First, what is BLE service?
  - Defined state information on a server
  - Standard defined services on the server are immutable
- What are BLE profiles?
  - Client defined use of server services
  - The profile could use multiple server services or services across multiple servers
  - Note: No specification of what the server must do in support of a BLE profile

BLE: Profiles

- What is the advantage of moving the responsibility of the profile from both end points to the client?
  - Enabling the server to be used in a “limitless” number of profiles that exist today and in the future
  - Minimize the code and responsibility of the server to save energy on the resource limited device



- For example:
  - A device provides the following services:
    - Temperature
    - Air quality
  - The client uses this devices services with a profile to provide an application with data on the temperature and air quality of a particular room in a building
  - Someday in the future, a new profile could be developed on the client that could take these device services and make it a fire or smoke alarm
- Moving the role to the client enables servers to be used in new roles that may not even be thought of today

BLE: Central (Discovering Devices)

- The first thing that a newly commissioned central device will do is to discover other devices
  - Passive Scanning: a central device passively listens to advertisement packets that peripherals are transmitting
  - Active Scanning: a central device, after hearing a peripheral, asks for more information
- If the Central device is only looking for what devices are around, such as when you open your mobile phone Bluetooth connections, it should only use passive scanning
  - Reduces the energy of the central and peripheral devices
  - If active scanning is used, the peripheral will need to listen to the central device and respond to request which will increase the radio active time consuming energy

BLE: Central (Discovering Devices)

- If the Central device is also populating a user interface with additional information on each device advertising, then active scanning should be used
  - Information that can be found in active scanning includes:
    - Name of the device
    - A unique number that identifies the device that can be used later to connect to the device
    - Discover some broadcast information data within the scan responses so that information that is being broadcasted can be obtained such as battery level or the current time

BLE: Central (Discovering Devices)

- During passive and active scanning, not only can the application obtain the contents of the advertising packets, but it can also receive the Received Signal Strength (RSSI) of these packets.
- If the Tx Power was included in the advertising packets, a basic estimate of the path loss and therefore an estimate of the distance between the device and central device can be determined
  - $path\ loss = TxPower\ - RSSI$
  - If the path loss is very small, between 0 and 20, the device is very close
  - If the path loss is very high, greater than 70, then the device is very far away
  - To eliminate multipath interference, these values should be averaged over a number of seconds

BLE: Central (Connecting to Devices)

- When initiating a connection, a set of connection parameters will need to be chosen depending on what the two devices are intending to do
- Typically, peripherals have a Client Preferred Parameters characteristic that gives a very strong hint to a central device about the type of connection parameters it prefers
  - Connect interval
  - Slave Latency
  - Etc
- When making the first connection with a device, this information is not available, so the central device should compromise between low power consumption and rapid characterization of a device

BLE: Central (Connecting to Devices)

- An example of a compromise would be a connection interval of 15mS to 30mS and a slave latency of 150mS
  - Allows both rapid collection of data about the peripheral using up to >60Hz connection intervals and a possible slave idle frequency of >6Hz
- The slave might request different parameters from those that an application on the central device has chosen after connection has been made
  - For example:
    - The peripheral may request a connection interval of 150mS and a slave latency of 750mS to minimize energy use
    - But, the application on the central device might require the data or state from the peripheral every 50mS, so the central sets up connection interval of 50mS and slave latency set to 0
    - The application will get the data it requires at the appropriate data rate, but the peripheral battery life will be negatively impacted

BLE: Central (What does this device do?)

- After connecting to the peripheral, the central device will need to discover what the device does using the following four procedures:
  - Primary Services Discovery
  - Relationship Discovery
  - Characteristic Discovery
  - And, Descriptor Discovery
- The first process is the Primary Services Discovery
  - These are the services that describe what the device does
  - For example:
    - If the device has a battery, the primary services would expose the Battery Service
    - If the device has a temperature sensor, the primary services would expose the Temperature Service
    - If the device had a temperature sensor within the battery, this secondary service of the battery would not be exposed through Primary Services Discovery