Internet of Things Systems Security

System Specification

UFCF8P-15-M

Luke Murray (19041865)

and

Jacob Williams (15008632)

# Initial Considerations

The specification for this coursework proposes the possibility of using different devices from the previously used Microbits, such as the Raspberry Pi or an Arduino. However, since thus far the Microbit has been utilized primarily it would make sense to continue using the Microbit. This also has the added bonus of experience working with an unconventional IoT device that has little documentation, giving a relatively fresh experience of IoT programming.

The second consideration will be which communication method to use with the Microbits. The choices being Radio or Bluetooth Low Energy. If using the Radio functionality it is possible to continue using the already familiar DAL runtime, however if one wishes to use BLE one would have to switch to using ARM Mbed. Both functionalities are provided by Lancaster University.

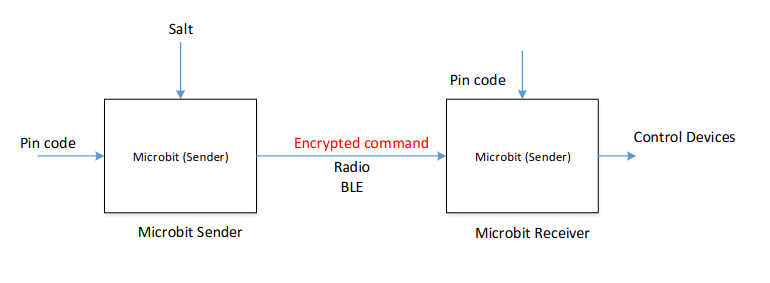
The Radio functionality is extremely simplistic, it works as one might expect. A device acts as the transmitter, another device idles using the DAL listen function to receive the communication and then one programs what happens as a result of what has been received. Lancaster University say that the Radio functionality is designed with “privacy in mind”, given that “there is nothing inherent to the protocol which can be used to identify you or your microbit”. However privacy doesn’t necessarily ensure security, given the open nature of the radio communication an attacker could technically intercept communications and even masquerade as either the sender or receiver if they so desired.

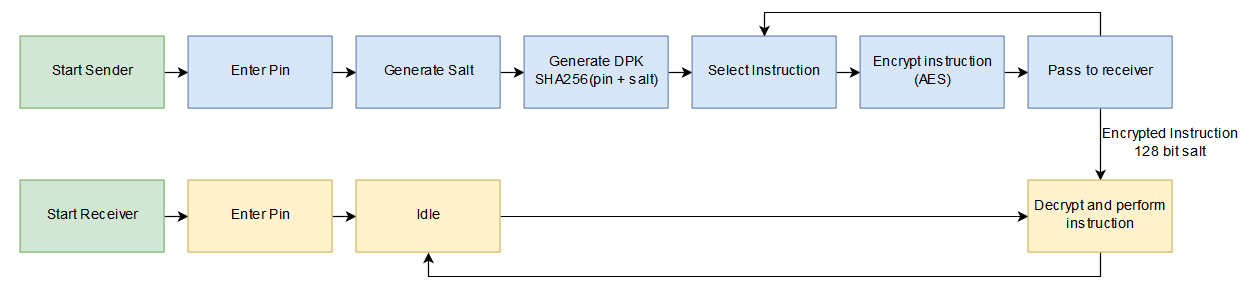
The Bluetooth functionality provides various security functions, including being able to pair with passkeys and including different protected communications. It also has whitelisting and the links between devices are encrypted by default. The draw back of BLE is that one would have to change the runtime and also develop for multiple different devices. As a result this method would be considered more difficult in the context of this project.

The method deigned to be used was Radio, its functionality sounds interesting and finding ways to incorporate security into a messaging functionality that is no way by default secure is an interesting prospect.

# Design

## Layman's Run Time

There is a example runtime laid out in the coursework specification, this being:  
The runtime being that the microbits are started, pins are entered on both microbits. The sender then generates a salt, which is combines with the pin code and encrypts in SHA256, giving us a 64 byte data protection key to use with the AES encryption later.

Above is a flow representation of the two roles the microbit can operate under, in theory one implementation can be created to perform both roles, where one simply chooses the desired role at the beginning of the runtime. The sender should be programmed to work like a hub, where it distributes commands to the recievers within range of it. The reciever should be designed in such a way that the number of recievers can be dynamic, anything running the reciever side of the program in range of the corresponding sender with the same pin should be able to receive the instructions.

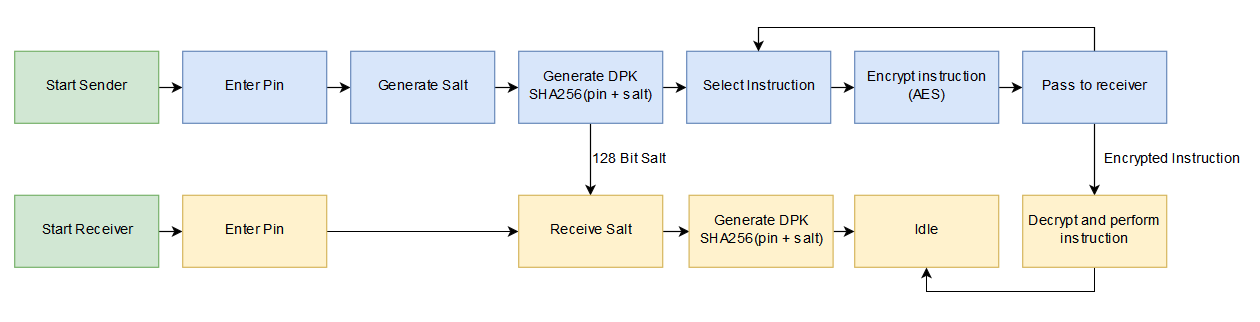
There is however a key flaw with the example runtime that stops it from being the basis of this project. The design implies that the salt is passed every time the sender sends an instruction which seems like a huge security flaw, as possible intruders intercepting the messages would see the repitition and possibly be able to breach the method of passing instructions.

Counteracting this would be a big undertaking, but an idea of how to reduce the potential entry of attack has been formulated, nicknamed “saltshaking”.

### Saltshaking

The concept of handshaking is an old and established protocol for linking two devices, effectively working by the sender sending an identifier, the receiver returning a confirmation of the identifier, and then the sender sending a confirmation of receiving the confirmation. This works to establish the connection and not require the passing of any extra identifiers after handshaking.

The Saltshaking implementation works under a similar basis. The sender distributes the Salt to the receivers before sending any instructions, so that when it comes to actually sending instructions there is no need to pass the salt multiple times.

In theory this implementation will reduce the potential of intercepting the salt and therefore potentially being able to breach the communication channel of the two Microbits, as all messages occurring after the Saltshake will be encrypted using the resultant DPK.

This method doesn’t counteract other possible security risks occurring from the factor of using the Microbit radio communication, such as intruders being able to masquerade as sender. But this method does reduce the potential effectiveness of an interception attack given that in essence the attacker has one chance to do it.

This method also creates another issue, the Saltshake can only in theory occur once, else it defeats its entire purpose. Because of this, if one unit in the cluster of devices loses its DPK (losing power, being manually reset) then the entire cluster will need to be re-initiated.

# References

Lancaster University (2016) *micro:bit Runtime.* Available from: <https://lancaster-university.github.io/microbit-docs/> [Accessed 17 December, 2019]

**System specification (10%)**

**(For group – all group member can use the same system specification)**

This document describes how the system will be built. It must therefore contain sufficient and appropriate detail. It can also be used to divide work up among the team members and to schedule different pieces of activity. A good specification:

* uses appropriate descriptive methods such as diagrams, sketches, storyboards, data dictionaries, etc.
* is internally consistent – ie information in one part does not contradict what is said in another
* contains sufficient detail for the system your group implemented, such as your solutions, protocols, state diagram, etc.