DAT 235

IoT Security

IoT assign 4 Bluetooth

Author:
Bendik Egenes Dyrli
Nikolai Kjærem Ellingsen
Jens Martin Håsæther
Mathias Solheim Jansen

Supervisor:
Geir Myrdahl Køien

2017

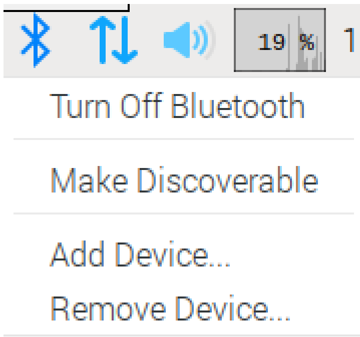
Contents

1 Introduction

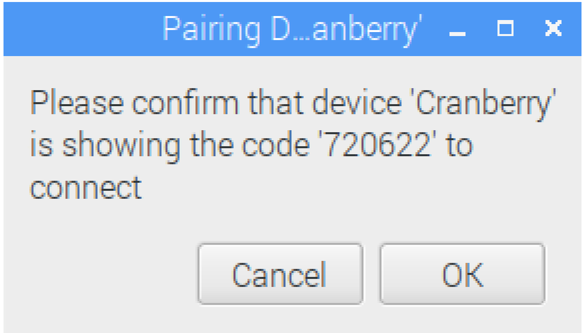
Bluetooth is a networking protocol which transmits data using low-power radio waves on the 2.45 gigahertz band. It avoids interfering with other devices by using a very weak signal of about 1 milliwatt. Which compared to a cellphones 3 watts is minuscule and only allows it to connect to devices approximately 10 meters apart. Eight devices can be connected within 10 meters without interference due to spread-spectrum frequency hopping. Each device uses 79 individual randomly chosen frequencies and changes between them regularly about 1,600 times per second. When two devices are within range of each other, they decide which one is the receiver automatically. A PAN(Personal Area Network) is setup between the two and they proceed to frequency hop in unison. This guide will cover how to connect to a Raspberry Pi Zero Wireless using GUI and terminal.

2 Setup guide with GUI

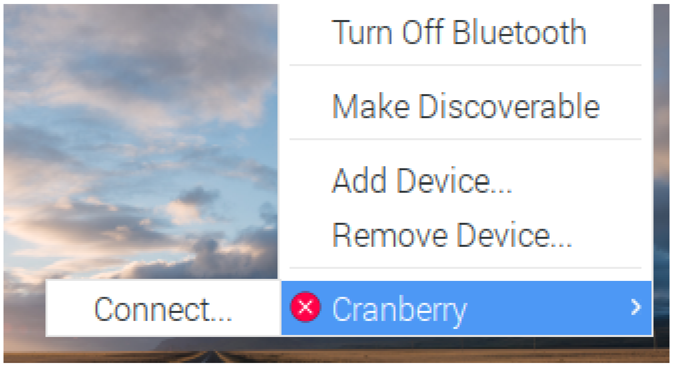
Connect to the Raspberry Pi Zero Wireless either with HDMI or through VNC. Afterwards, there should be a GUI with a toolbar on the top.



In this toolbar, you can select the Bluetooth icon. You will get 4 options; turn off/on Bluetooth, Make discoverable, Add device and remove device. If Bluetooth is not turned on, turn it on. After that, you will either need to make it discoverable to connect from another device or select add device if you want to connect from the Raspberry Pi Zero Wireless. Click on ok if prompted and the device should be visible if you click on the Bluetooth icon again.

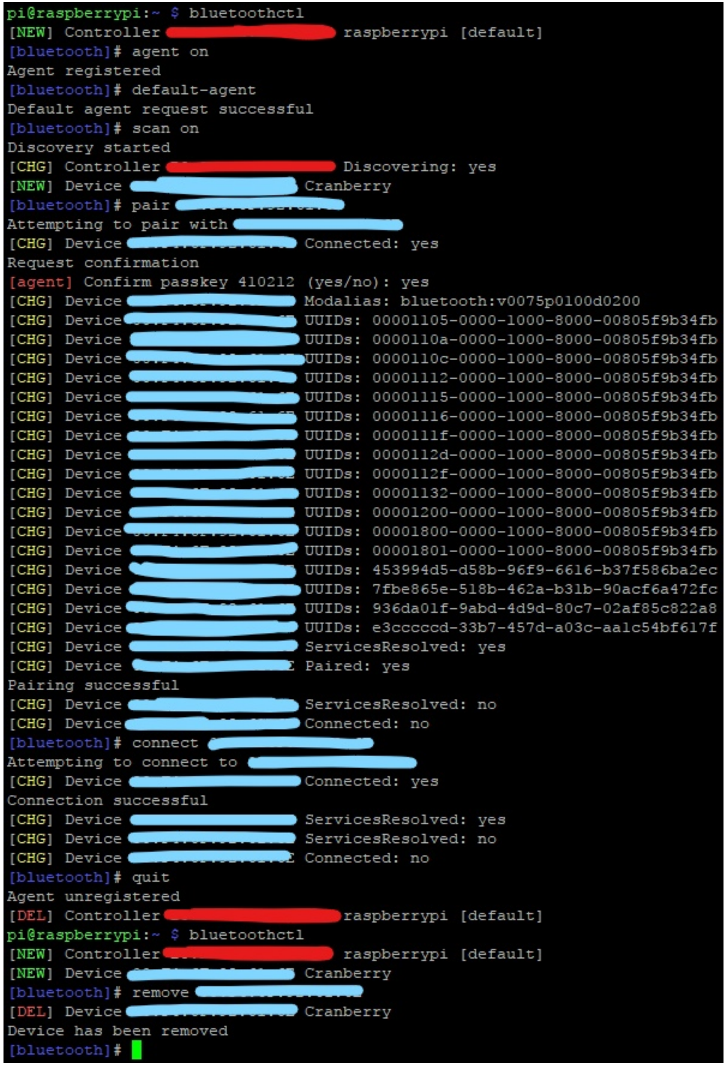


Please confirm that device 'Cranberry' is showing the code '720622' to connect



3 Setup guide with terminal

Type sudo bluetoothctl in your terminal, enter your superuser password if prompted. This will start the Bluetooth terminal application allowing you to control your Bluetooth easily. Now type agent on and press enter, then type default-agent and press enter again. If you want to check nearby devices, type scan on and press enter. Adresses will now be listed in the following format XX:XX:XX:XX:XX:XX. If you see the device you want to pair, write pair followed by the address of your device. Now if you on the otherhand want to connect from a device to the Raspberry Pi Zero Wireless, type discoverable on and press enter. This will make your Rapsberry Pi Zero Wireless discoverable by other devices for 3 minutes. To remove a device, enter remove and the device id. If you want to exit the bluetooth application, enter quit and press enter or press CTRL+D. Also as a sidenote, remember that pressing TAB, will auto complete your commands or text inputs in BASH. This is very useful when typing your device id.

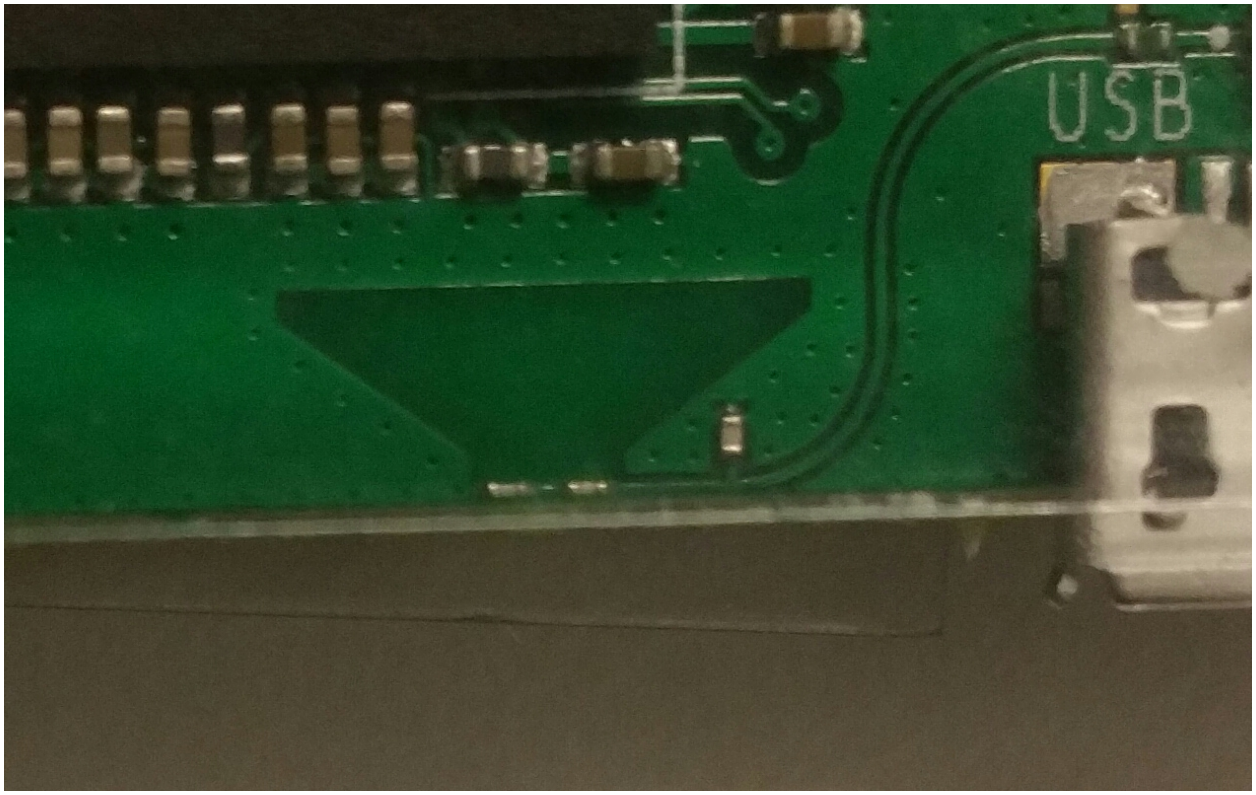


```
pi@raspberrypi:~ $ bluetoothctl
[NEW] Controller [redacted] raspberrypi [default]
[bluetooth]# agent on
Agent registered
[bluetooth]# default-agent
Default agent request successful
[bluetooth]# scan on
Discovery started
[CHG] Controller [redacted] Discovering: yes
[NEW] Device [redacted] Cranberry
[bluetooth]# pair [redacted]
Attempting to pair with [redacted]
[CHG] Device [redacted] Connected: yes
Request confirmation
[agent] Confirm passkey 410212 (yes/no): yes
[CHG] Device [redacted] Modalias: bluetooth:v0075p0100d0200
[CHG] Device [redacted] UUIDs: 00001105-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 0000110a-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 0000110c-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 00001112-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 00001115-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 00001116-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 0000111f-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 0000112d-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 0000112f-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 00001132-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 00001200-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 00001800-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 00001801-0000-1000-8000-00805f9b34fb
[CHG] Device [redacted] UUIDs: 453994d5-d58b-96f9-6616-b37f586ba2ec
[CHG] Device [redacted] UUIDs: 7fbe865e-518b-462a-b31b-90acf6a472fc
[CHG] Device [redacted] UUIDs: 936da01f-9abd-4d9d-80c7-02af85c822a8
[CHG] Device [redacted] UUIDs: e3ccccd-33b7-457d-a03c-aa1c54bf617f
[CHG] Device [redacted] ServicesResolved: yes
[CHG] Device [redacted] Paired: yes
Pairing successful
[CHG] Device [redacted] ServicesResolved: no
[CHG] Device [redacted] Connected: no
[bluetooth]# connect [redacted]
Attempting to connect to [redacted]
[CHG] Device [redacted] Connected: yes
Connection successful
[CHG] Device [redacted] ServicesResolved: yes
[CHG] Device [redacted] ServicesResolved: no
[CHG] Device [redacted] Connected: no
[bluetooth]# quit
Agent unregistered
[DEL] Controller [redacted] raspberrypi [default]
pi@raspberrypi:~ $ bluetoothctl
[NEW] Controller [redacted] raspberrypi [default]
[NEW] Device [redacted] Cranberry
[bluetooth]# remove [redacted]
[DEL] Device [redacted] Cranberry
Device has been removed
[bluetooth]#
```

4 Raspberry Pi Zero Wireless Antenna

Unlike the Raspberry Pi 3 with a two-sided Broadcom standard design with a chip-type antenna. The Raspberry Pi Zero Wireless uses a single-sided layout with a PCB antenna. To elaborate further, A Pi 3s antenna is surface mounted and the Pi Zero's antenna is a resonant cavity which is achieved by etching away layers of copper in the different layers of the PCB. The reason for doing this is obviously due to the space constraints in the Raspberry Pi Zero Wireless.

First and foremost the antenna consists of a ground plane that can be located easily next to the USB port due to it's triangular shape. This is the resonance cavity where radio waves interact with the free space at an exact frequency. Two capacitors at the top of the triangle(bottom of picture) capture the radio signal. As a result, a lot of work payed off to make the Raspberry Pi Zero Wireless possible within it's form factor.[1]



5 Bluetooth security

Just like any other wireless communication, Bluetooth is not without it's security flaws. Automatic connection is a great ”quality of life” enhancer, but is equally useful for sending date without your permission. Authorization and identification is therefore needed. The first step is to only allow trusted devices to function without asking permission. Secondly, the user should be prompted to accept connections and file/data transfers. Furthermore, the devices should only be discoverable for a limited period of time. Bluejacking for example, works by sending a ”business card” over Bluetooth. If the recipient allows this contact to be added, they may now receive messages that are automatically opened since they are being sent from a known contact. Bluesnarfing allows access to all information on the targets phone. Bluebugging on the other hand, allows full control of the targets phone without their knowledge. All of these can generally be avoided by turning off discoverable mode on your device. As technology progresses, so do the tools used to break them.

References

[1] WIRELESS WONDER: THE NEW PI ZERO W ANTENNA DESIGN [Online] https://www.raspberrypi.org/magpi/pi-zero-w-wireless-antenna-design/ [Accessed:11.October 2017]