Hardware Workshop Attendee Manual

Damien Cauquil (@virtualabs)

I. Introduction

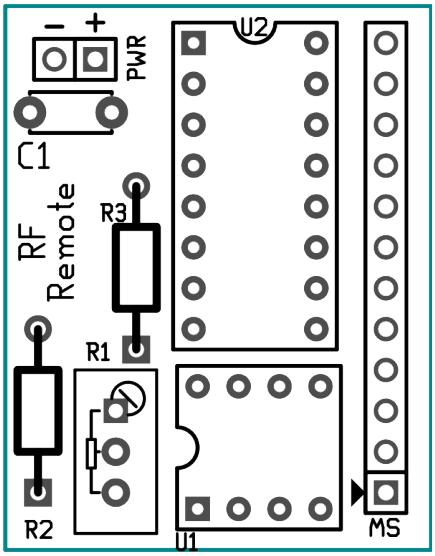
During this workshop, you will turn a basic RF remote found in a wireless chime into an hardware bruteforce device able to make every similar wireless chimes ring without knowing their secret codes.

This hack is based on an additional PCB that will be soldered as a kind of « shield » for the RF remote, and will modify its behavior. This PCB is pretty generic, and may be used to modify other remotes as well.

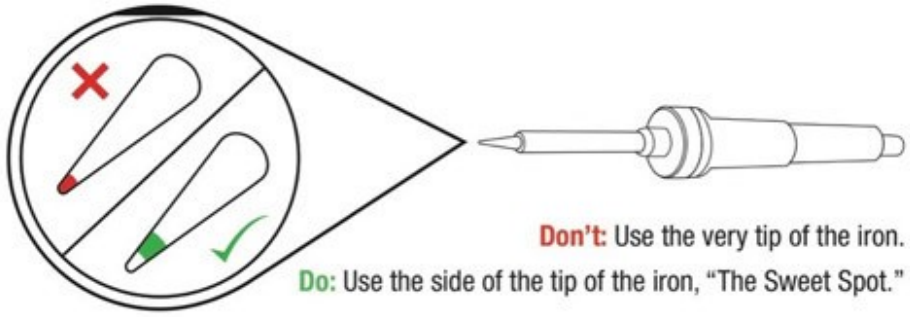
II. Bill of Materials

Reference	Description
PCB1	Printed Circuit Board for NSC#2 workshop
R1, R2	680 Ohms resistors
C1	47uF polarized capacitor
D1, D2, D3, D4, D5, D6	1N4148 diodes
U1	NE555P
U2	CD4040BE
Wires	Wires

III. Layout diagram



IV. Soldering tips



Don't: Use the very tip of the iron.

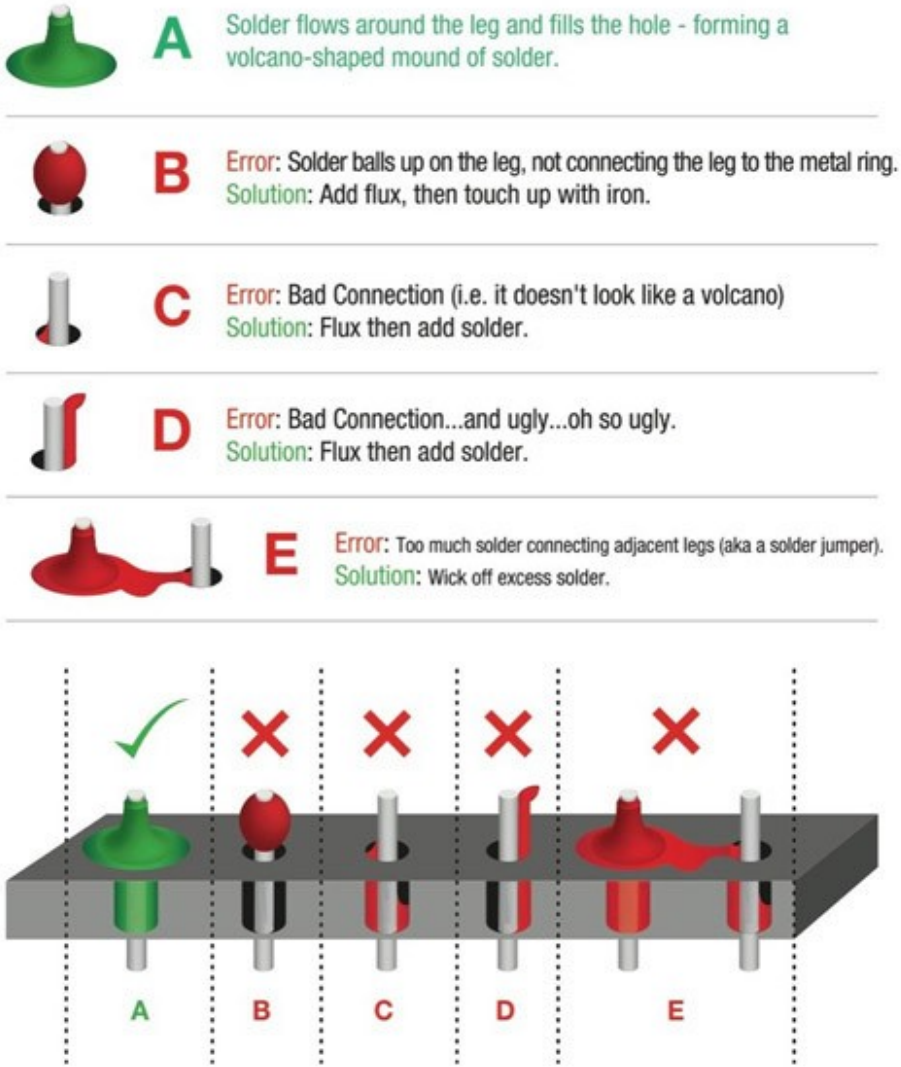
Do: Use the side of the tip of the iron, "The Sweet Spot."

Do: Touch the iron to the component leg and metal ring at the same time.

Do: While continuing to hold the iron in contact with the leg and metal ring, feed solder into the joint.

Don't: Glob the solder straight onto the iron and try to apply the solder with the iron.

Do: Use a sponge to clean your iron whenever black oxidization builds up on the tip.



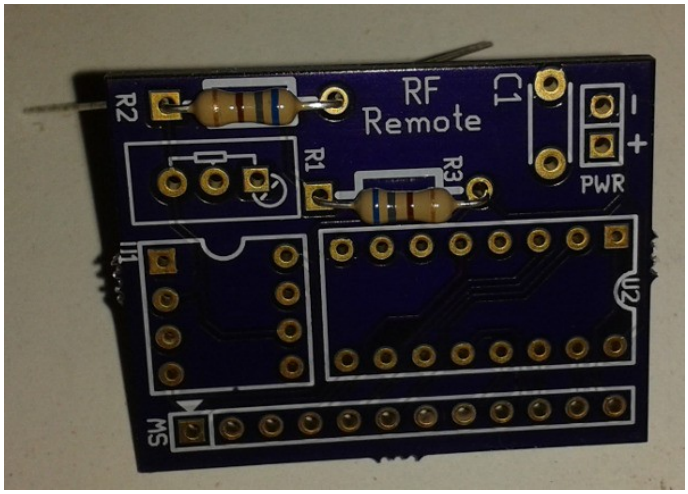
(Image from Sparkfun, https://learn.sparkfun.com/tutorials/how-to-solder---through-hole-soldering)

V. Build instructions

V.1. Resistance is not futile !

First of all, you need to solder the R1 and R2 resistors on the PCB, do not worry about which one is R1 or R2 because they are both the same. Solder them one by one, following these steps :

1. use a pair of pliers to fold the resistance pins in order to fit in the holes
2. put the resistor in place, it must rely on the silkscreen (side of the PCB where « R1 » and « R2 » are visible)
3. slightly fold the resistor legs to make them point to the outside of the PCB
4. prepare some solder and your soldering iron
5. apply the tip of your iron on both the PCB's pad and the resistor leg at the same time
6. bring some solder on the iron tip, it will drop down and fill the hole
7. remove your iron
8. check your solder joint, fix it if required
9. cut the legs right above the solder



Steps 5 to 7 must be performed quickly, as your iron will heat the component. If you heat too much, your component may be damaged or destroyed. Usually, your soldering iron tip must not be in contact with your component more than 4 seconds in order to keep it safe.

V.2. U2 is not only available in iTunes, eh.

Once the resistors soldered, you have to solder U2, a.k.a CD4040BE. This is a binary counter provided in DIP16 package. DIP16 packages are like bugs : a lot of legs and difficult to catch.

You may have noticed the presence of a slight marker at the top of this component : this will help you while positionning this latter on the PCB. You may use a tiny screwdriver to slightly fold the legs in order to make it fit in the PCB, but be very careful : these damn legs are easily damaged.

Once in place, follow the same procedure :

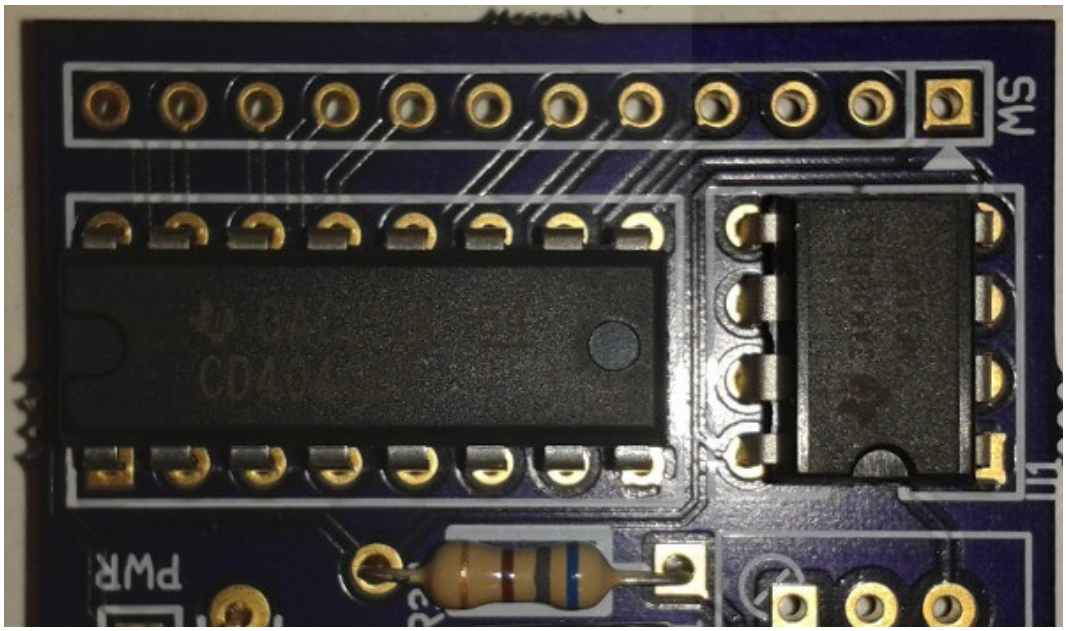
1. prepare some solder and your soldering iron
2. apply the tip of your iron on both the PCB's pad and one leg at a time
3. bring some solder in the joint, it will drop down and fill the hole
4. remove your iron
5. check your solder joint, fix it if required, then go next pin

You may have to wait a while between two solders in order not to make the component heat too much. The temperature of your soldering iron may also be adjusted if too hot (if possible).

V.3. U1 must also be soldered

U1, a.k.a NE555P, is a DIP8 package with only 8 pins. Use the same tricks as for U2 to make it fit inside the PCB, and solder the same way :

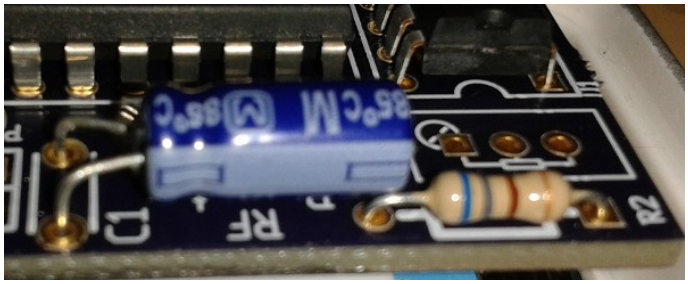
1. prepare some solder and your soldering iron
2. apply the tip of your iron on both the PCB's pad and one pin at the same time
3. bring some solder on the iron tip, it will drop down and fill the hole
4. remove your iron
5. check your solder joint, fix it if required, then go next pin



V.4. Time (to solder this damned) capacitor !

Capacitor C1 is polarized, that means you MUST care about polarity. And of course, since this workshop was designed by a lazy guy (yeah, me), there is no *minus* sign on the PCB to give a clue on how to place it. Well, the *minus* of the capacitor (the white stripe on it) must face the border of the PCB.

There is some space to fold the capacitor legs and make it consume less room on the circuit board, so keep a 4 or 5 millimeters clearance and fold the legs at 90°. Place the component like this :



Then, solder the same way as before :

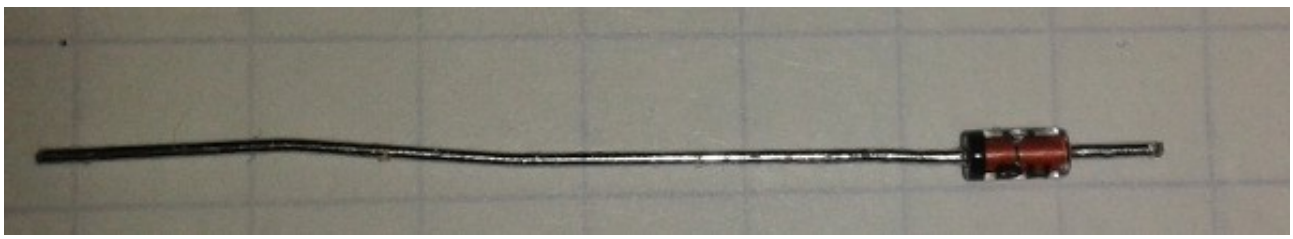
1. prepare some solder and your soldering iron
2. apply the tip of your iron on both the PCB's pad and one of the C1 leg at the same time
3. bring some solder on the iron tip, it will drop down and fill the hole
4. remove your iron
5. check your solder joint, fix it if required

Be careful, heating a capacitor too much make it EXPLODE. And of course, we will not tolerate any injury.

V.5. Soldering the diodes, part I.

Diodes are going to be used as wires to communicate with the underlying circuit board. This is not convenient, but a very good way to save space.

Cut each diode cathode and left a 4 or 5 millimeters clearance, as shown below :

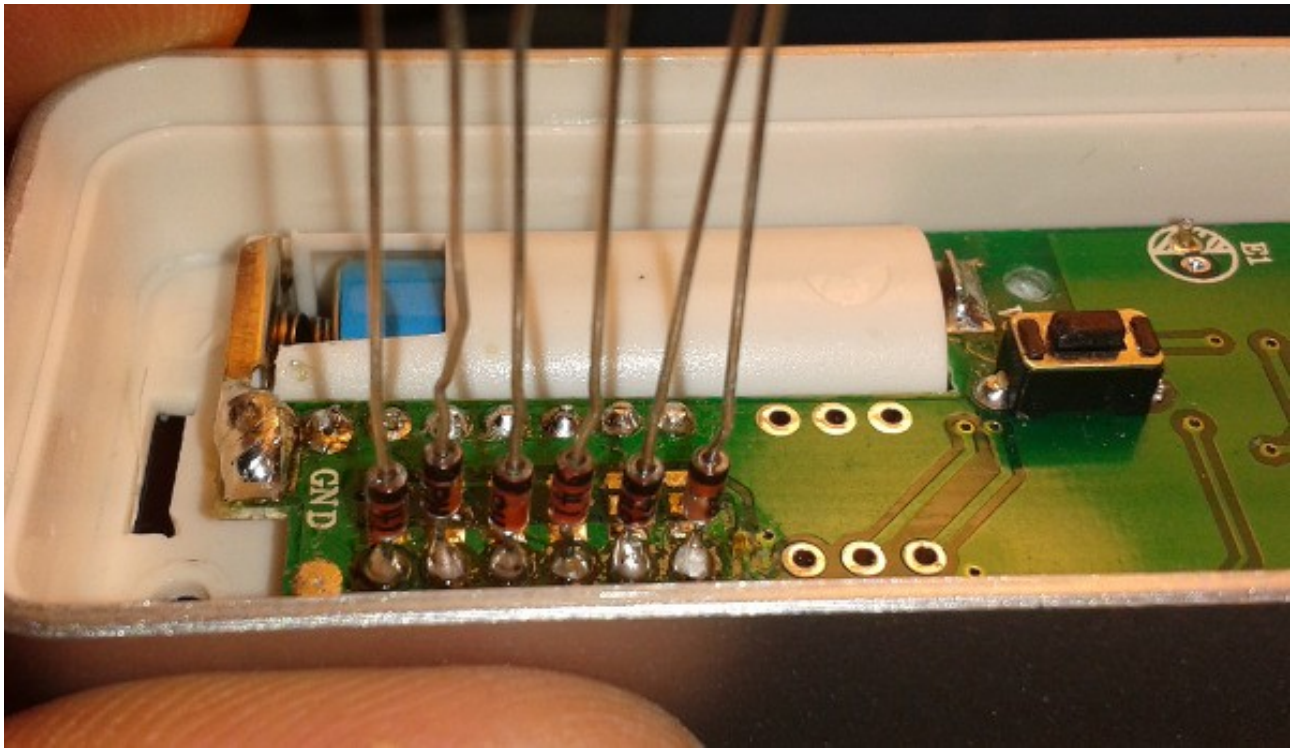


Then, add some solder on the microswitch legs (on the original circuit board) with your soldering iron : be careful not to link a leg to another one.

Eventually, pick diodes one by one and solder them vertically :

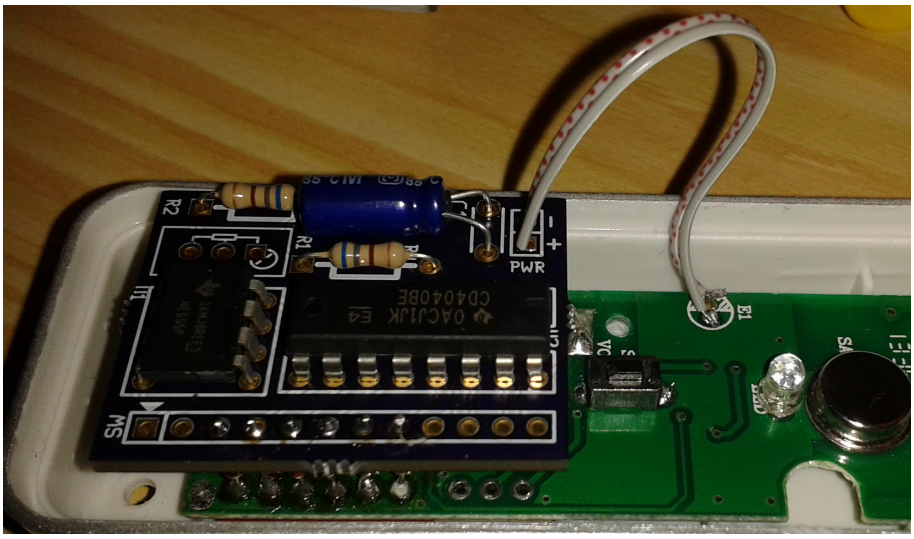
1. Place your iron tip on the solder on the pin and heat
2. Place vertically a diode and make it touch the melt solder
3. Remove your iron tip and wait for the solder to cool down
4. Check your solder joint

Repeat for each diode, and at the end you may get this :



V.6. And now, get the power

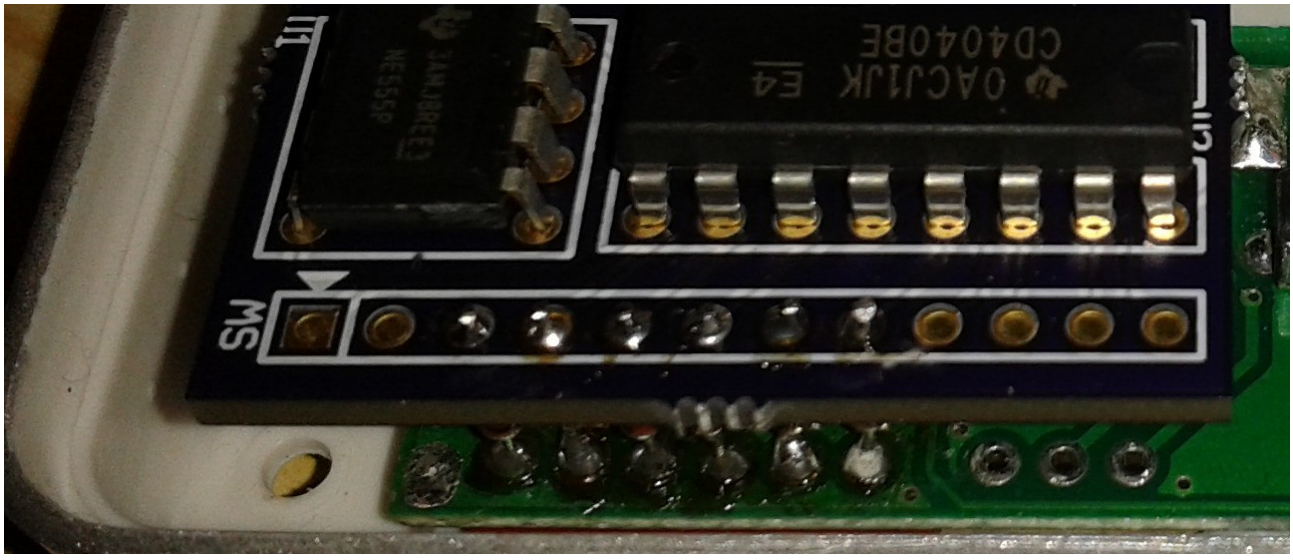
Take a wire, solder one end to the ground, take another wire and solder one end to Vcc.



Solder the ground wire to the PCB (power, *minus*) and then the other (*plus*). This will power your board.

V.7. Soldering the diodes, part II.

Once the wires soldered on the PCB, place it above the soldered diodes and make them go in the right holes as shown below :



This last step is a bit difficult, but must be done : solder the diodes on the component side of the PCB, use a third hand in case of extreme difficulty or shaking issues.

And you're done with soldering !

V.8. Testing your hacked RF remote

Time to test your hacked RF remote ! Push the tactile switch, the LED will light on. Wait some seconds (around 20~30 seconds) for the chime to ring. Enjoy the power of old-school electronics !

VI. Thanks

The author would like to thank the NoSuchCon orgs for their help, and especially :

- Joffrey Czarny
- Nicolas Ruff
- Geoffrey Bertoli
- Jonathan Brossard