RFID sniffer kit

Introduction

The RFID sniffer is a simple analog electronic circuit which can detect the presence of 13.56 MHz RFID tags. These tags are commonly used in all kinds of plastic cards like access badges, bank cards, library cards, loyalty cards and so on. Also many other objects may carry RFID tags without you knowing it. Books, toys, and even clothing might be tagged. Carrying tagged objects with you can reveal your identity or whereabouts to anyone equipped with the appropiate tools to read RFID tags.
The RFID sniffer helps you identify which objects are tagged, and which are not.

Kit contents

- Printed circuit board
- SMD components in 4 separate bags
  - Bag 1
    1x 0Ω jumper (L1)
    2x 33pF capacitor (C1, C2)
    4x 10kΩ resistor (R1, R2, R4, R6)
  - Bag 2
    2x 220pF capacitor (C3, C4)
    2x 470Ω resistor (R3, R7)
    1x BAS32 diode (D1)
  - Bag 3
    1x 1nF capacitor (C5)
    1x red LED (D2)
    1x BC817 NPN transistor (T1)
    1x MCP6541 voltage comparator (IC1)
  - Bag 4
    1x 100nF capacitor (C6)
    1x 10kΩ potentiometer (R5)
    1x pushbutton switch (S1)
- CR2032/1HF lithium battery
- Plastic sleeve with zip-lock
- Lanyard with metal clip

Required tools

- Soldering iron (preferably temperature controlled) with fine tip (1-2 mm)
- Good quality solder with flux core, 0.5 mm (preferably lead-free, with 2-3% silver)
- Sharp-tipped tweezers
- Solder wick (2-3 mm)
- Flat long-nose pliers
- Wire cutter
- A steady hand!

Optional tools

- Miniature screwdriver (for adjusting the sensitivity)
- Flux pen (helps in soldering)
- Cotton swabs + thinner (for cleaning the pcb after soldering)
- Magnifying lamp (highly recommended!)

SMD soldering tips

Soldering SMD components requires some experience, and a steady hand, but it can be learned by anyone. SMD components are very small, and therefore heat up quickly when touched by the tip of a soldering iron. Never hold the soldering iron on a SMD component for more than 2 seconds!

The easiest way to solder these small parts is to first apply a little bit of solder to one solder pad on the circuit board, and then hold the SMD part in place with tweezers while briefly heating up the solder pad without applying more solder. Once the part is fixed on one side, the other side, or other pins, can be soldered by applying a little bit of solder with the soldering iron in one hand, and the solder wire in the other hand. The trick is to first heat the solder pad, then apply solder until it melts, remove the solder, and remove the soldering iron. All this should happen well within 2 seconds. Be sure to regularly wipe the tip clean on a wet sponge.
Some people prefer to use a flux pen to improve the wetting of the solder on the pads. In my experience this is not needed when you use a good quality solder (with 2-3% silver) and a fine, clean soldering tip.

If you made a mistake, or applied too much solder, wait a few seconds until the joint cools off, then remove excess solder with solder wick. Place the solder wick at the joint, and place the tip of the soldering iron on the solder wick, which will then suck up the solder. Don't remove the soldering iron before the wick, or it will stick to the joint. If the wick gets full of solder, simply cut it off.

Again, prevent overheating of the components and pads. If it doesn't work like it should rightaway, wait a few seconds and try again, after wiping the soldering tip on a wet sponge.

Assembly instructions

Work on a clean, smooth surface, not above a carpeted floor! You will certainly loose the tiny SMD parts when accidentally dropped. The kit contains no spare parts.
All SMD parts are packed in four separate bags. The capacitors are unmarked and have a light grey or light brown body. The resistors have a white body, black on the top side, and are marked with their value in very small text.

The easiest part to solder is the relatively large 0Ω jumper (L1), so that's where we start. Since this part is a bit bigger than the other parts, it doesn't burn so easily, and you can use it for soldering practise.

After placing the jumper, apply a little bit of solder to one solder pad of all the other parts. It doesn't really matter which side. Then solder all the parts one value at a time. Open only one bag at a time, and solder the same value components one after the other. So first C1 and C2 (both 33 pF), then R1, R2, R4 and R6 (all 10 kΩ), and so on.

The diode and the LED have to be mounted in the right orientation. The diode has a black stripe on one side (the cathode). This side should point to the right.

The LED is a bit more tricky, because it is very hard to see which side is the cathode. If you look closely, you can see a faint dot in the middle of the LED. It is not exactly in the middle however, it is slightly to one side. This side is the cathode, and should be on the

right, just like the diode. The bottom has a green stripe with a stub. This stub should point to the same direction.

If you have a multimeter, you can verify the LED orientation by selecting the diode test function on the multimeter, and the LED should light up when the red (positive) lead is on the left side (anode) and the black (minus) lead on the right side (cathode).

The transistor, comparator and potentiometer only fit the pads in one way, so that should be no problem. Make sure the leads are aligned properly with the pads. The 3 pins on one side of the comparator are likely to get shorted together, but it's easy to remove the excess solder with solder wick afterwards.

The switch can be mounted in either direction, and might require a bit longer for the solder to flow, since it's a much larger component which takes some of the heat away.

Lastly, the battery. The battery is mounted in a large hole in the pcb to reduce the height. The battery has legs for through-hole mounting, so we have to modify them a little bit. First squeeze the battery upside down (legs up) in the hole. This is most easliy done by placing the battery upside-down on a table, with the legs up. Then position the hole in the circuit board over the battery, and firmly press down the board. Align the terminals of the battery with the solder pads, paying attention to the polarity. The polarity is marked on the board. The positive terminal of the battery is the side with the engraved text, and since the battery is upside down, is facing the bottom. After pressing the battery in the hole, it should be flush with the bottom of the circuit board.

Use a small screwdriver or pliers to fold the legs flat onto the solder pads and cut off the thin part of the legs. Make sure you don't short-circuit the battery with your tools! Solder the folded and trimmed legs to the pads, applying a generous amount of solder. This will take a bit longer than with the small components. Pay good attention to the polarity, double check before soldering! Also make sure you don't touch the yellow insulator sleeve with the soldering iron, it will melt and cause a short circuit.

After soldering all parts, clean the board using a cotton swab dipped in thinner. The soldering flux leaves a residue which can't do much harm, but it just looks dirty.

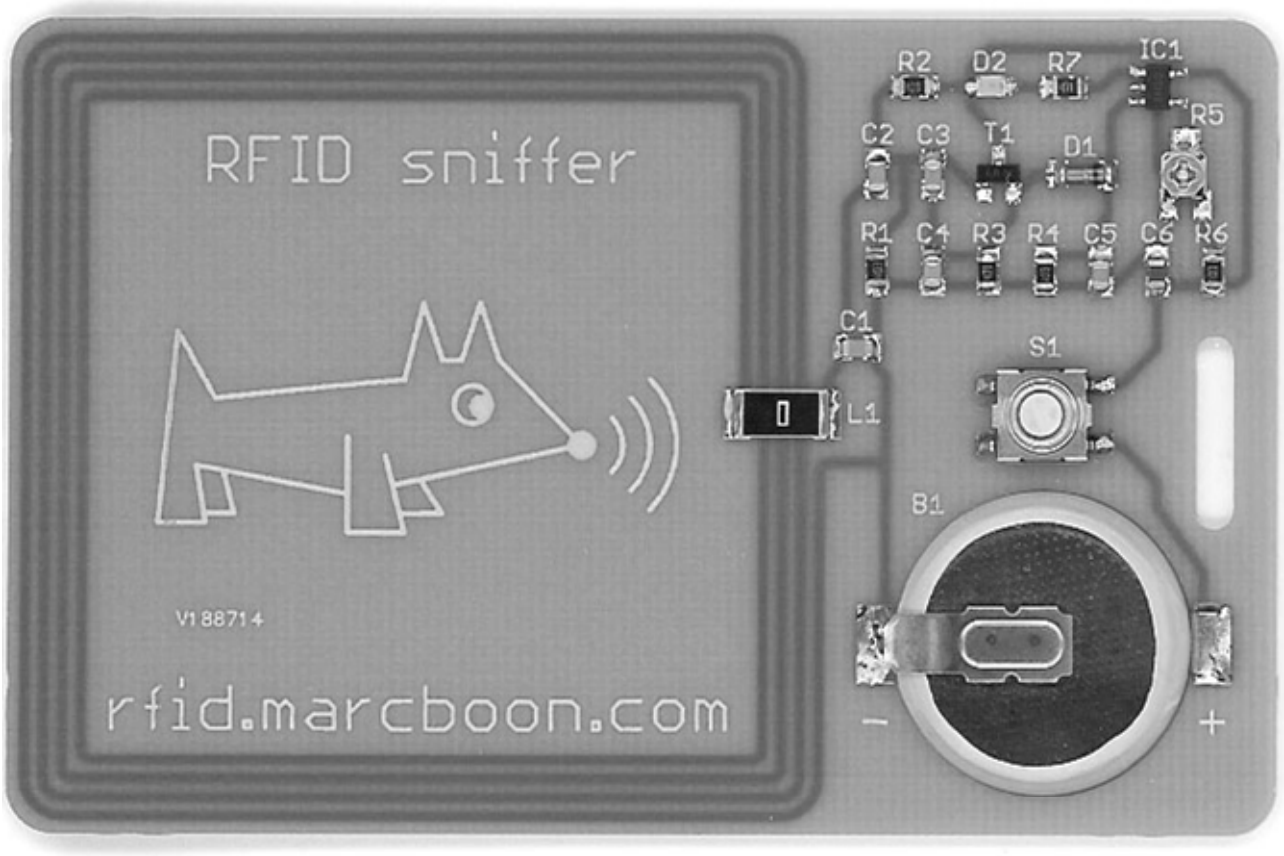
Testing

Obviously you will need a RFID tag for testing. Many newer passports have one build in, and so do many library cards, public transport cards and access badges for schools and offices. If you're not sure you have a RFID tag, try a metal surface. The RFID sniffer also reacts if held very close to a metal surface, since this absorbs RF energy like a RFID tag does.

To use, press the button while holding the sniffer close to a suspected object. If the LED turns on while holding it close, and off while moving away, the object is tagged.
If the LED is always on, or never on, try adjusting the potentiometer using a miniature screwdriver. Normally no trimming will be nescessary.

Happy sniffing!

Finished board



Schematic diagram