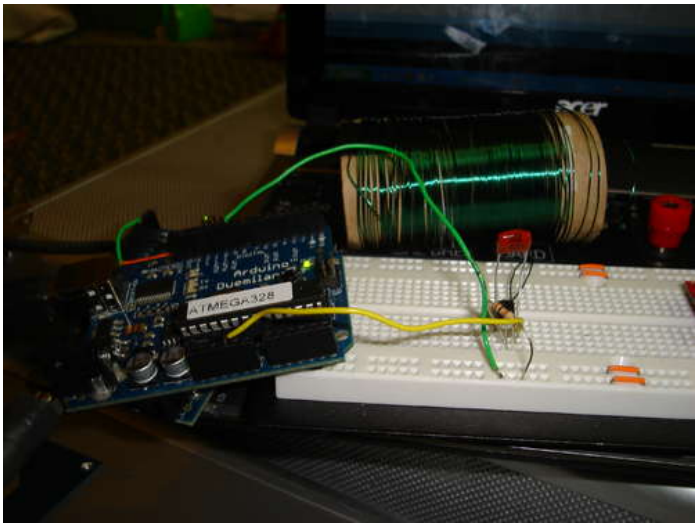
Stupid Simple Arduino LF RFID Tag Spoofer

by **sketchsk3tch** on April 9, 2010

Table of Contents

Intro: Stupid Simple Arduino LF RFID Tag Spoofer

RFID tags are all over the place. They're used in building access control systems, passports, inventory tracking . . . This instructable will show how you can use an Arduino and a few simple components (wire coil, transistor, capacitor, resistor) to make a device that can spoof an 125 KHz (low frequency) RFID tag. This is version 1, so there are many enhancements that can be made, but this version is stupid simple, yet it works. I did this in a few hours without much previous knowledge of RFID and without any fancy equipment (like a radio tuning hardware or an oscilloscope . . .I guess an oscilloscope is fancy, I need to pick up one of those).



step 1: Parts

Parts:

*Some enamel coated solid core copper wire (I used the green spool from the 3 spool set Radio Shack carries).

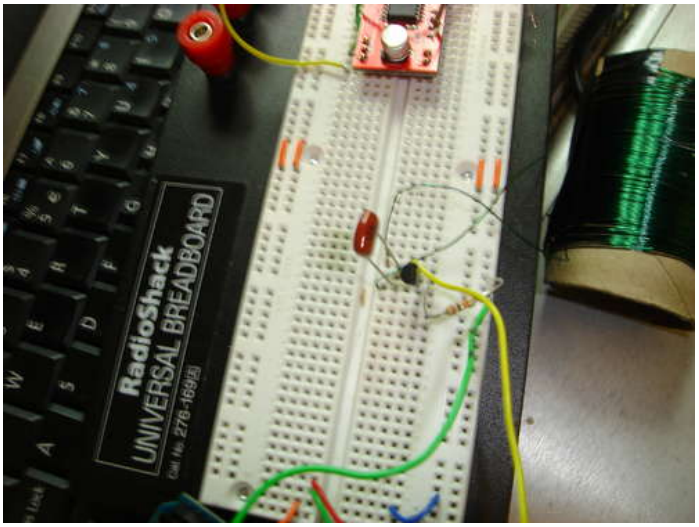
*A NPN transistor, I used a 2N3904

*A 10 K Ohm Resistor

*A 10 nF capacitor (0.01 uF). I'm using a Metalized polyester film cap I got from Radio Shack, others should work though

*A toilet paper roll to wind the wire on

I tested my circuit using a Parallax RFID serial reader connected to a second Arduino



step 2: RFID background

A passive RFID tag has a coil and a chip with data on it. An RFID reader has a coil in it that has a coil in it that creates a varying electronic field (in this case 125 KHz), which is called the carrier signal. When the tag is close to the RFID reader then the magnetic field powers the chip on the tag, which then responds by tuning and detuning its own antenna. This all works on the principle of inductive coupling, to learn more about his see www.rfid-handbook.de/rfid/types_of_rfid.html

125 KHz cards use manchester encoding to encode the data to send it to the reader. Manchester encoding basically takes the XOR of the bit that needs to be transmitted and the clock value. So if the clock value is low (0) and the value to transmit is 1 then it would be 0 XOR 1 which is 1. This has to be done on every clock cycle. For more information on manchester encoding see en.wikipedia.org/wiki/Manchester_code .

step 3: The Data

You can either download the code below, or get it here: www.scribd.com/doc/30215336/RFID-Faker-Code

The serial number of a tag is sent over using a fairly simple protocol.

It starts by sending 9 one's

Then it sends 10 sets of 4 bits, then one parity bit (it's using even parity)
Then it sends "column" parity bits (even parity of the rows in the previous step)
Last it sends a 0 stop bit

So an example looks like this:

(start bits)
111111111

(10 rows of data - the card serial number)
(the first 4 bits are the data, the last is the even parity bit)

11110
10100
10001
11000
10010
11101
11110
00000
00011
01010

(then it sends the column parity bits, even parity of the rows above)

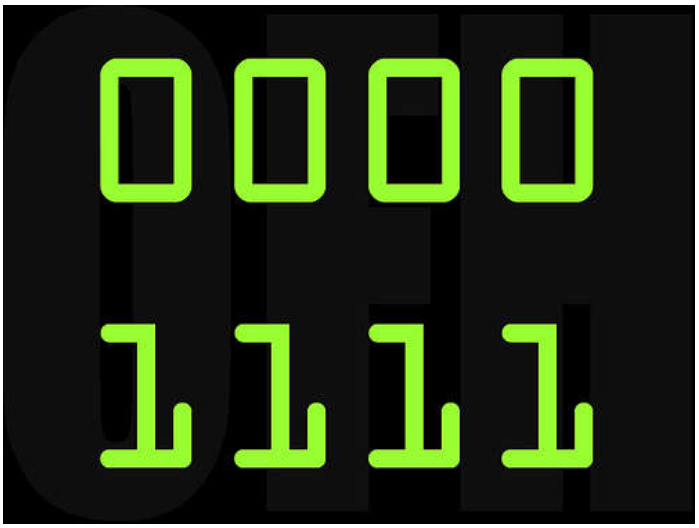
1101

(last a 0 stop bit)

0

See the pdf in the first link in the references section for more details on this

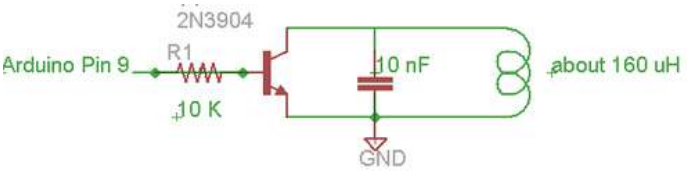
Image provided by Flickr user at www.flickr.com/photos/kurtisscaletta/2473469841/ and used under the creative commons license.



step 4: Building the circuit

You need to create a coil that's about 150 to about 162 uH (different sources say it should be different values). To determine how many winds to do you can use an induction calculator like the one here www.crystalradio.net/cal/indcal2.shtml . I used the green spool from the Radio Shack set of wires and wound it about 133 times around the toilet paper roll (I did this both by working with a calculator and some trial and error, I have no tuning equipment). You probably want to leave a little extra wire in case you need to wind some more to get your antenna tuned right.

After you have your coil you can connect it to your circuit. The schematic is pretty easy. Just connect pin 9 on the Arudino to a 10 K Ohm resistor, then to the base of the transistor. Next you can put your capacitor between the collector and emitter of the transistor. The emitter also needs to be connected to ground. Next connect the coil the the emitter and collector of the transistor.



step 5: The code

The Arduino now needs to tune and detune the antenna. When pin 9 is low then the antenna is tuned (sending out a "high" signal). When the pin is high then it sends power to the base of the transistor. This reduces the resistance between the two ends of the coil, which "detunes" the antenna. We just need to do this in the right sequence to send data to the reader. The code generates a tag ID that's 10 hex F's. If that's what you get in your reader then you know it's working.

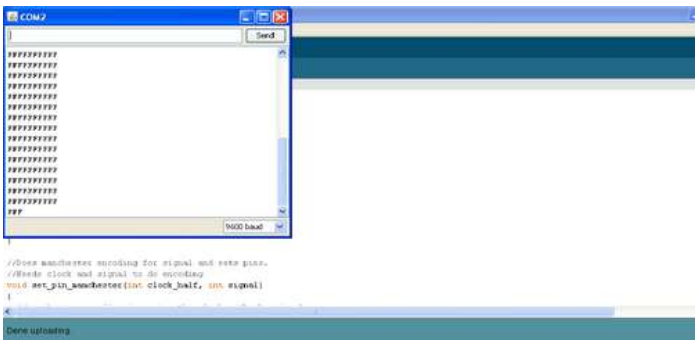
File Downloads

rfidFaker.pde (1 KB)
[NOTE: When saving, if you see .tmp as the file ext, rename it to 'rfidFaker.pde']

step 6: Testing

To test the circuit hold the antenna right up to the reader (go ahead and touch it to the reader for the first test), if everything's right you should see the tag ID you're hoping to see. If not (and you're sure the sketch is uploaded properly and the circuit is connected correctly) start adding and removing winds from the coil and retesting it. It should be somewhere in the 120-140 range with the green Radio Shack wire I used.

Once it's working at really short ranges (touching the reader) you can mess with the coil some more to tune the antenna better and you should be able to get a range of a few inches.



step 7: The Video

First I hold up a real tag to the reader, and you'll see by the screen behind it that the tag ID is read and displayed on the screen behind it. Next I hold my coil up and the reader sees it as a tag and reads the serial number off it.

step 8: Elephants in the Room

This project does have a few deficiencies that should be mentioned. First, since the RFID emulator runs on it's own clock instead of using the one from the magnetic field the reader creates not every serial ID broadcast is received by the broadcaster. This isn't a huge deal because in my experience they end up matching up close enough every about every second or two. If you wanted to modify this so it could brute force tag IDs it might be more important that every tag ID is broadcast correctly.

The second issue is the form factor of the antenna. It should be easy to modify this though by simply collapsing the coil. At that point though you'll need to use a different calculator that does multi-level coils to figure out how to wind it.

Last, there's the range. By experimenting with the coil winds and the capacitor you should be able to get a few inches of range. More range would probably need some type of an amplified coil.

The image for this step is from www.flickr.com/photos/exfordy/123900378/ used under the creative commons license.

step 9:

References

PDF on a similar project, good discussion of how it all works and schematic
mrl.cz/projects/rfid/rfid.pdf

Similar project, including C code
www.alexanderguthmann.de/en/emulator.html

An RFID tag that's just a small Microchip uController and a resistor
micah.navi.cx/2008/09/using-an-avr-as-an-rfid-tag/

A similar project, also a reader
www.cq.cx/prox.pl

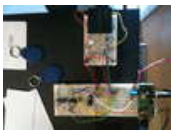
School project, cool ideas, missing some details though
www.dennislambing.com/senior-design-rfid/

Related Instructables

How to connect Arduino and RFID by otaviousp

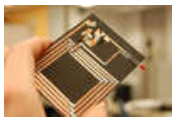
Magnetic stripe card spoofer by powerpants

AVR/Arduino RFID Reader with UART Code in C by nevdull



Arduino RFID Door Lock by pcmofo

How to block/kill RFID chips by w1n5t0n



RFID Reader Detector and Tilt-Sensitive RFID Tag by nmarquardt

RFID pet feeder by landmanr

Control a Schlage electronic deadbolt with an arduino! by quadmasta

Comments

13 comments **Add Comment**

evanwehrer says:
I'm gonna make a shield for this!

Apr 26, 2010. 12:56 PM **REPLY**

yaba says:
Hi, nice work!!
Now tell me, we could use some PIC or anyother device right?
I wonder if we could use Bus Pirate + some script in Python or Perl?!?!?!?
Thanks

Apr 20, 2010. 4:17 AM **REPLY**

sketchsk3tch says: Apr 20, 2010. 6:28 AM **REPLY**

Anything that can power the transistor on and off with a 256 microsecond delay between them should work. So yeah, a PIC should work. I bet the Bus Pirate could as well. I've got one of those on order at Seeed, but I ordered it with their new logical analyzer so it won't ship until that does.

lras says: Apr 19, 2010. 12:12 AM **REPLY**

Shouldn't the sixth line "11100" be "11101"? (Zero-happy again? :-)

sketchsk3tch says: Apr 19, 2010. 6:19 AM **REPLY**

You're right, thanks for pointing that out. It should be fixed now. Let me know if you notice anything else.

lras says: Apr 19, 2010. 12:14 AM **REPLY**

Or perhaps it should be "11110" to make the column party correct.

Learndy says: Apr 16, 2010. 1:28 PM **REPLY**

Coilcraft offers RFID transponder coils of different inductance and range. From inductance you can calculate the capacitor. They are much more compact than a TP-roll. Even smaller than an empty roll. ;-) They are not very expensive and Coilcraft supplies free samples.

--
Airspace V - international hangar flying!
http://www.airspace-v.com/ggadgets for tools & toys (MODIS image og the day will be repaired soon)

iBurn says: Apr 15, 2010. 11:44 AM **REPLY**

Which Arduino board are you using? Or rather, which would be the most appropriate for this application on a budget? Thanks in advance
--
IBurn

hollenback.c says: Apr 15, 2010. 12:19 PM **REPLY**

That's an Arduino Duemilanove (ATmega 328). They're about $30 from SparkFun, $35 from the Makershed. If you wanted something cheaper, you could get an arduino clone of some kind, like the boarduino ($18?), but they get a little more complicated. You'll probably do best with a Duemilanove. Good luck.

spyguy99 says: Apr 13, 2010. 7:07 PM **REPLY**

Thank you for this! I've been looking all over for an Arduino based RFID spoofer, and now here it is!

robomaniac says: Apr 13, 2010. 9:16 AM **REPLY**

Normally, to peek people interest, it is recommended to put the video on the main page. Because that video is a resumer of your entire instructable.

Also in your video, a better view of your computer screen would of been nice.
A video of the screen capture (Camstudio) at the same time of the video would of been nicer.
More work in the editing but that would of ensure more views on youtube and instructables.

Keep it up, I like the idea.

takatomon says: Apr 11, 2010. 5:52 AM **REPLY**

Isn't 10 nano farads .01 micro farads not .001?

sketchsk3tch says: Apr 11, 2010. 7:48 AM **REPLY**

Thanks takatomon, you're right, I got 0 happy it looks like.