Hardware Hacking For Us Dumb Software Guys

ARDUINOS

Disclaimer

- Any material shared with any other talks is purely coincidental.
- I’m sure I thought of using it first by the way.

Hardware Hacking For Us Dumb Software Guys

ARDUINOS

Hardware hacking is daunting for many computer hackers

- complex components and circuits
- cost
- steep learning
- lack of goods information
- But I want to make cool stuff!

*Image Source - Flickr

Microcontrollers mix hardware and software

- You can drop code on the chip
- Can do the same things as complex circuits
- You can reprogram them

Google Trends

*Source Google Trends

Arduinos

- Open-Source hardware platform
- All-in-one prototyping board
- Easy to learn language
- Free, Open Source IDE
- Strong Community Backing
- Cheap (around $30)

Like a hardware equivalent of a scripting language

What's an Arduino?

Arduino Duemilanove

- ATmega328p
- 14 Digital I/O pins
  - 6 are PWM Pins
- 6 Analog pins
- 32 KB Flash
- 16 MHz

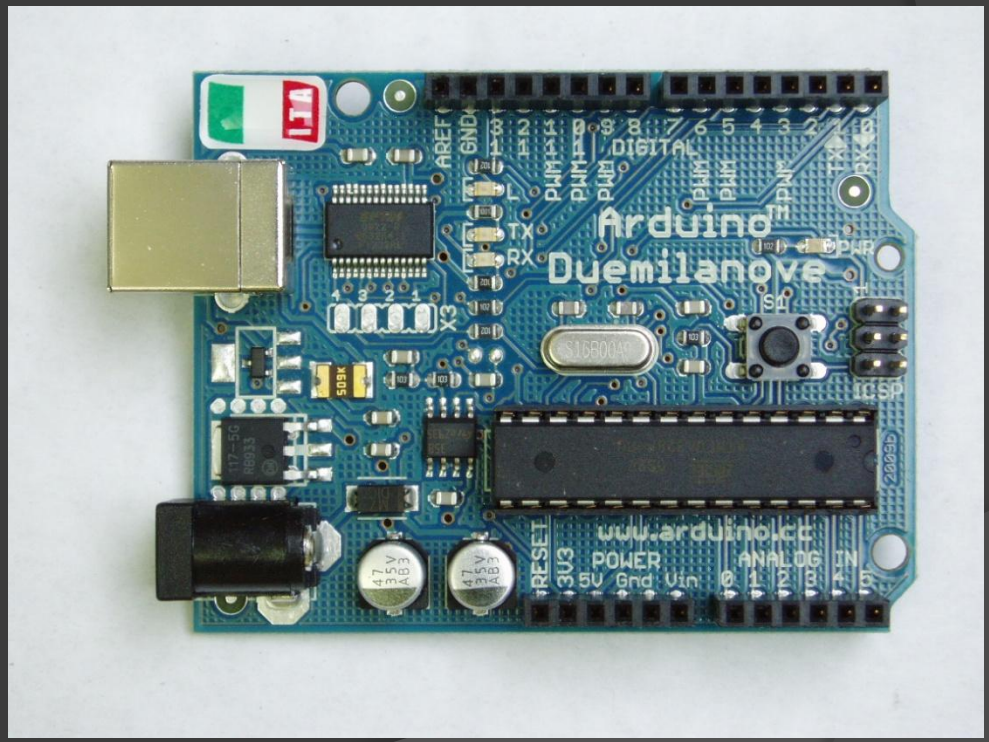


*Image source – Wikipedia.org Arduino

What else is an Arduino?

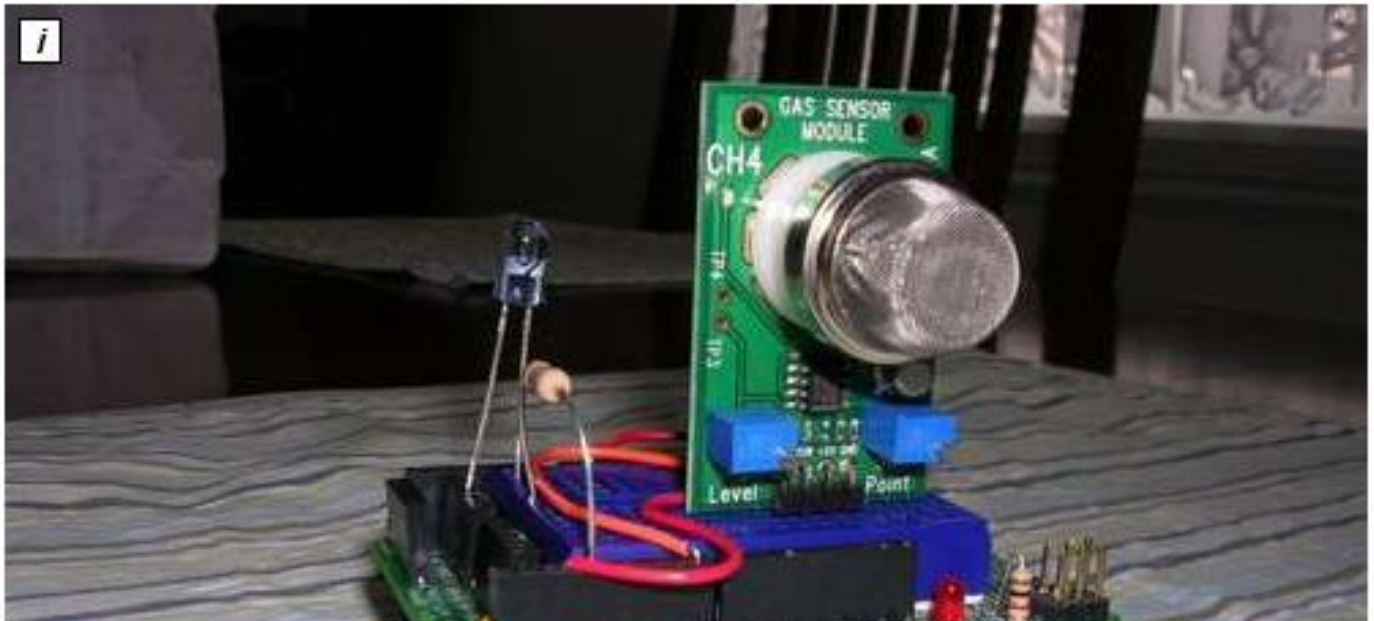
- Many other Arduino compatible boards
- Some boards are only IDE compatible, others are also pin compatible
- Arduino Mega
  - Sparkfun's Arduino Pro and Mini
  - Evil Mad Scientist Diavolino
  - Freeduino, Seeeduino
  - Fio
  - Teensy
  - Lilypad
  - Ardweeny & Bare bones
  - Maple
  - Butterfly Uno

General Purpose

intro Fart Operated Random Channel TV Remote

OK, I know that sounds weird, but bear with me for a moment. My Pops really enjoys two things channel surfing and 2) farting.
So one day I was over at http://hackaday.com/ and read about a guy who used his Arduino to tur TV on and off with one of those brainwave reading headsets. Then later on that same day I was here at Instructables and a fellow had made an office chair that twitters every time he farted. So got to thinking and decided to mash those two hacks into one remote that changes the TV to a random channel every time he tutes!
Plus, if you throw it in a plastic enclosure and hide it between the couch cushions; you've got a purdy dang good prank!

(As an aside, I've done some internet searching and I think this might be the first flatulent opera history of the world... I'm happy to be an innovator.)



Not for every project

- Expensive when you want to make a lot of devices
- Not incredibly powerful
- No parallel computing (have interrupts)

Image Source - Flickr

Blink LED

```
#define ledPin  13;    // LED connected to digital pin 13

void setup()   {
   pinMode(ledPin, OUTPUT);
}

void loop() {
  digitalWrite(ledPin, HIGH);   // set the LED on
  delay(1000);                  // wait for a second
  digitalWrite(ledPin, LOW);    // set the LED off
  delay(1000);                  // wait for a second
}
```

Shields

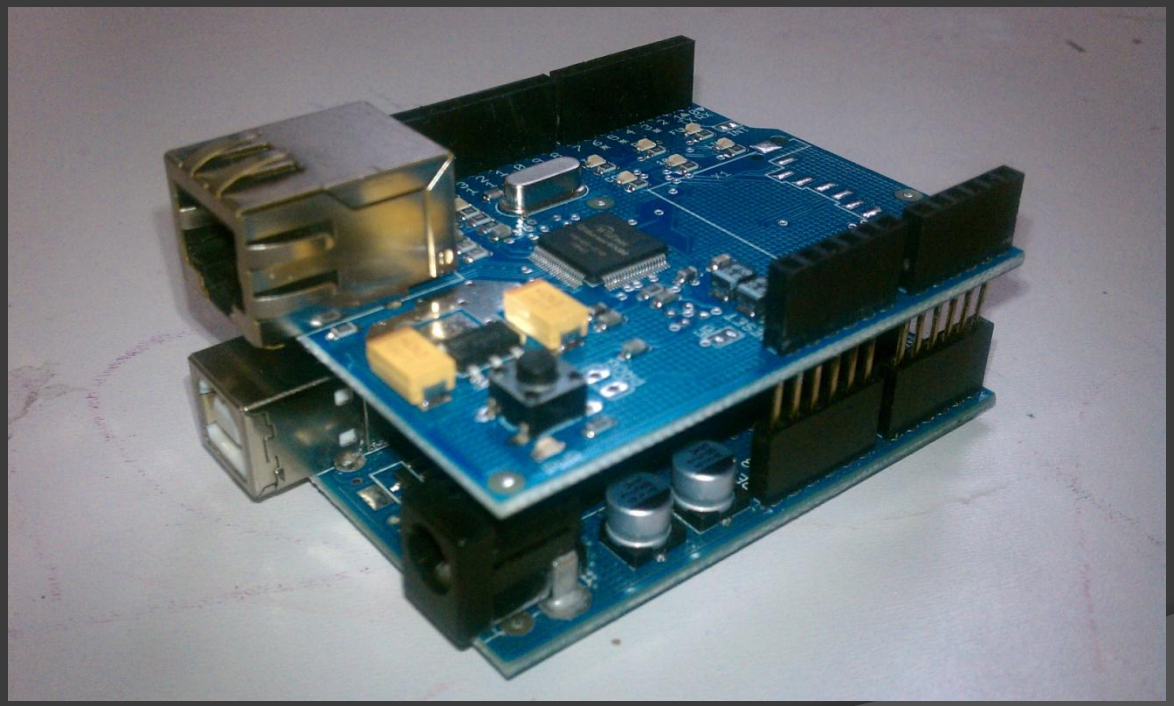
- Fit on top of an Arduino
- Add extra functionality
- Many are stackable

Using Available Shields

- Many shields are available, including:
  - Ethernet Shield
  - Xbee Shield
  - Motor Shields
  - Wave Shield
  - Nixie Tube Shield
  - LCD Shield
  - Cellular Shield
  - . . .
- Advantage – no tools necessary

Ethernet Shield

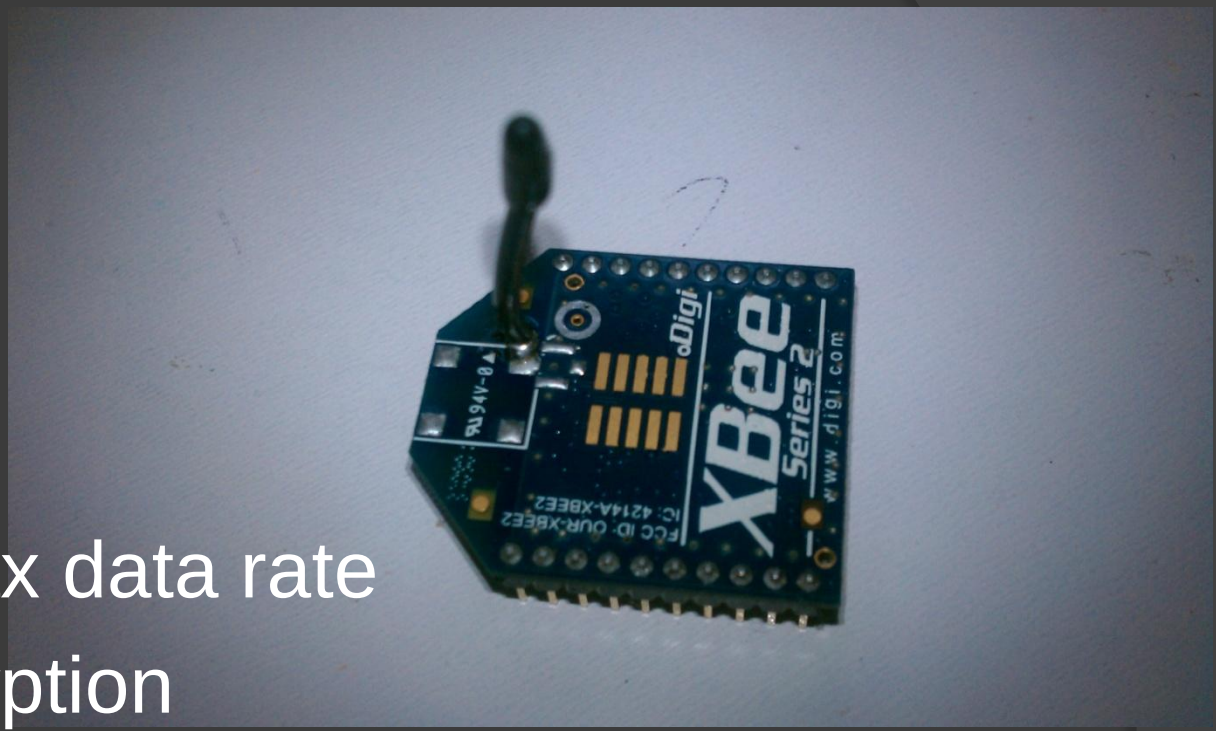
- Can function as a client or server
- Up to 4 simultaneous connections



Port Scanner

```
byte hosts_to_scan[] = { 192, 168, 1, 1 };
int last_octet = 1;

void loop() {
  hosts_to_scan[3] = last_octet;
  last_octet++;
  if (last_octet > 255) { last_octet = 1; }
  for(int i = 1; i < 1028; i++)   {
    Client client(hosts_to_scan, i);
    if(client.connect())     {
       //The port is open
    }
  }
}
```

Xbee



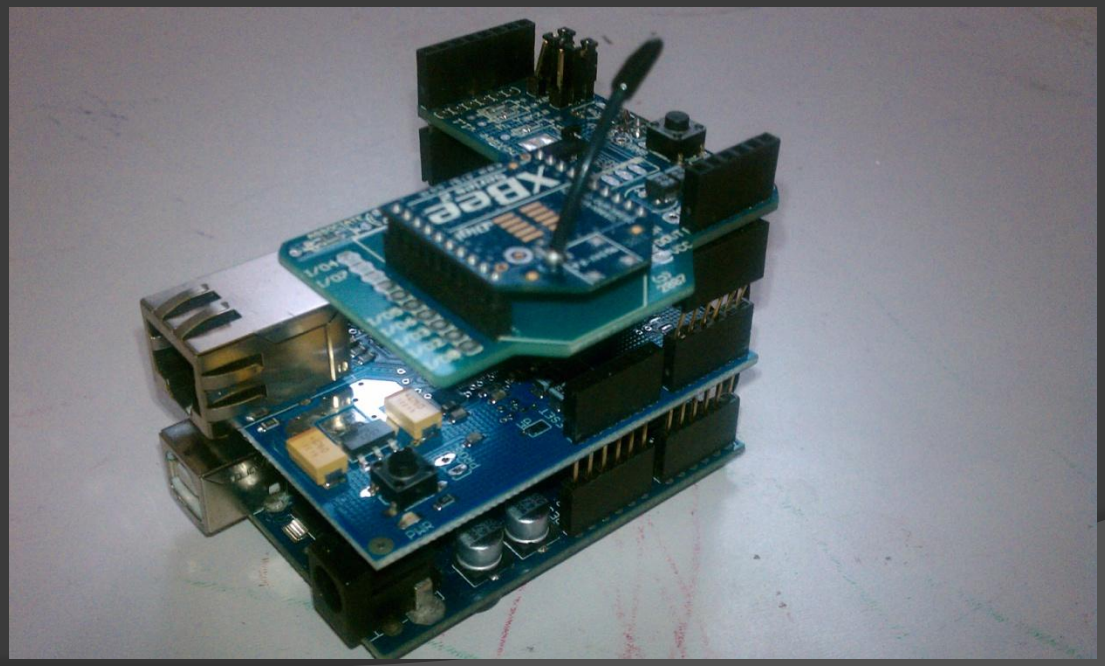
- 2.4 Ghz
- 250 kbps max data rate
- 128 bit encryption
- From a few hundred feet to several miles in range

Xbees and Security

- Can be used for out of band communication
- Even though they run on 2.4 GHz it's unlikely they'd be detected during a war driving assessment (not 802.11)
- Reprogram your Arduino remotely
- Triangulation?

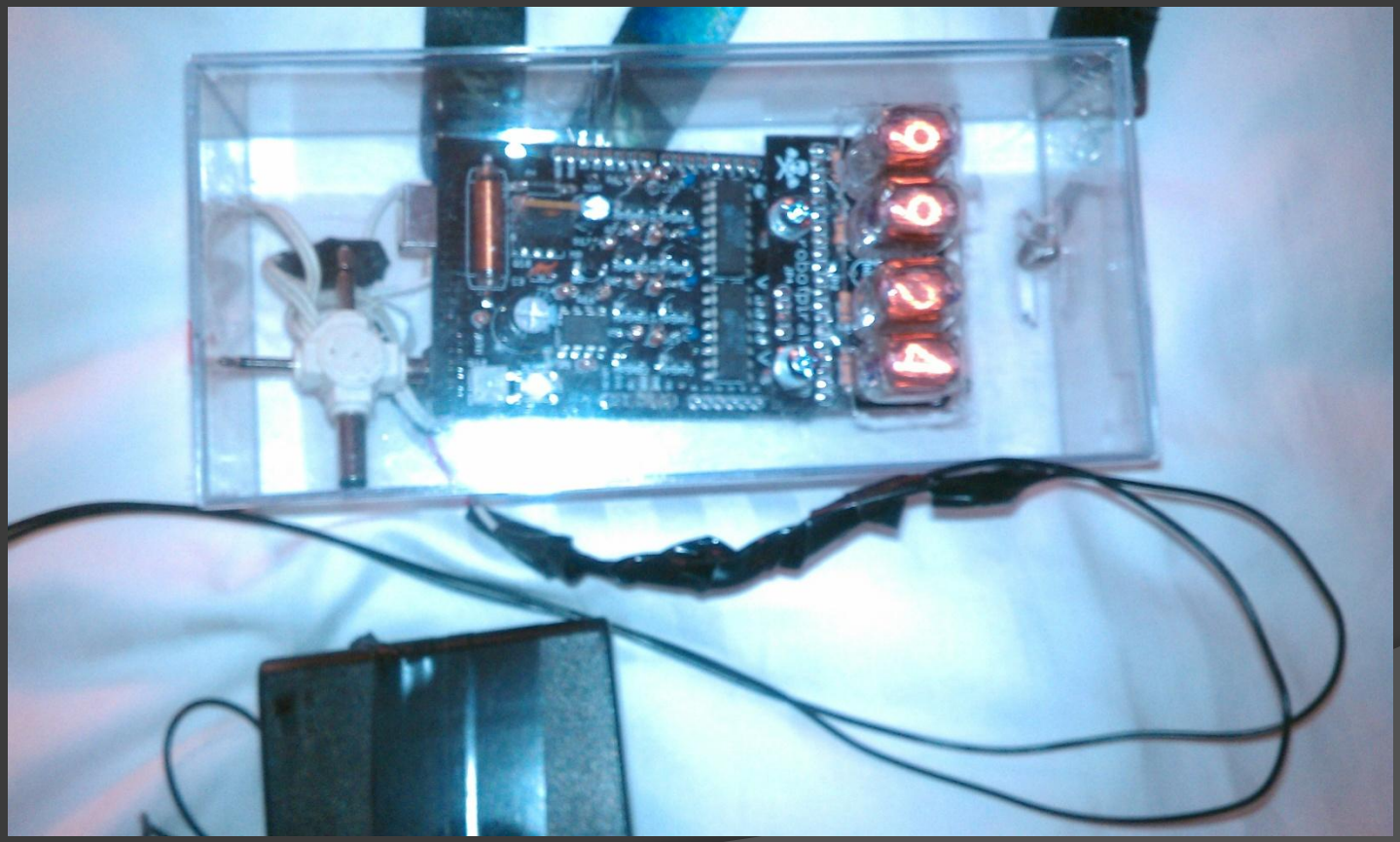
Xbee Shield and Ethernet Shield Together

- Xbee traffic difficult to detect
- Small Device
- Put it inside a network device



Nixie Tube Shield

- Used it to make my Nixie Badge



Making your own Shields

- You can use a proto shield, custom PCB or multipurpose PCB
- You'll need a soldering iron and possibly other tools

Reading From Pins

- Digital Reads
  - Returns 1 if positive voltage on pin
  - Returns 0 if there is no voltage on pin
- Analog Reads
  - Returns an integer between 0 and 1023

Electronic interface to devices are like form fields

- They are expecting a certain type of input
- Give them something else
  - Fuzzing
  - Specially crafted

Lie Detector

- DISCLAIMER: Be careful running voltage through people

Image Source – Flickr

Circuit

- Wire from 3.3 v on the Arduino, connected to a piece of tin foil
- Wire to an analog read pin connected to a second piece of tin foil
- 10 k Ohm resistor going from analog pin above to ground

Using the Lie Detector

- Wrap tin foil around two different fingers
- Code polls the analog read pin every few seconds
- When a person lies perspiration generally increases, so resistance decreases
- Reduced resistance will cause a higher value on the analog read pin

Lie Detector Code

```
#define lieDetectorPin 2;

void setup() {
   Serial.begin(9600);
}

void loop() {
  Serial.println(analogRead(lieDetectorPin));
  delay(5000);
}
```

Not Perfect

- Doesn’t really read if a person is lying or not
- Any emotional response will give the same reaction as a lie
- Real lie detectors also look at heart rate, breathing rate, etc.

Laser Tripwire

- Laser goes across a doorway
- Pointed at a photoresistor connected to an analog read pin on the Arduino
- Alerts when low light level

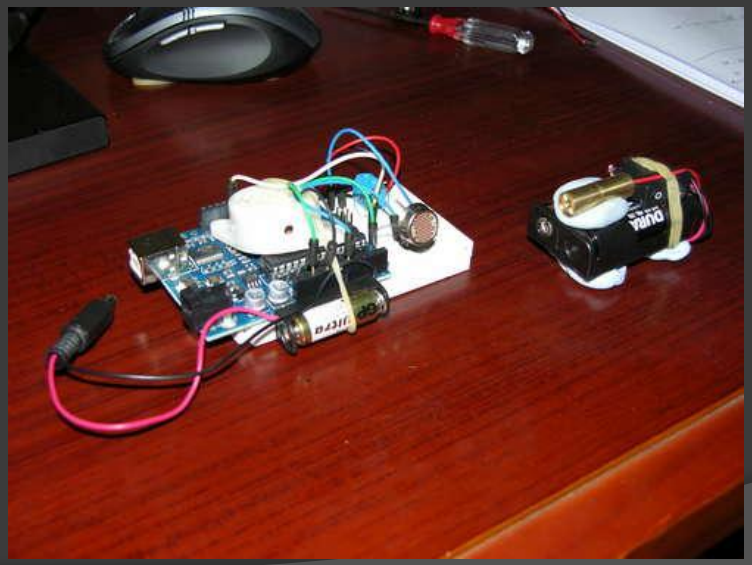
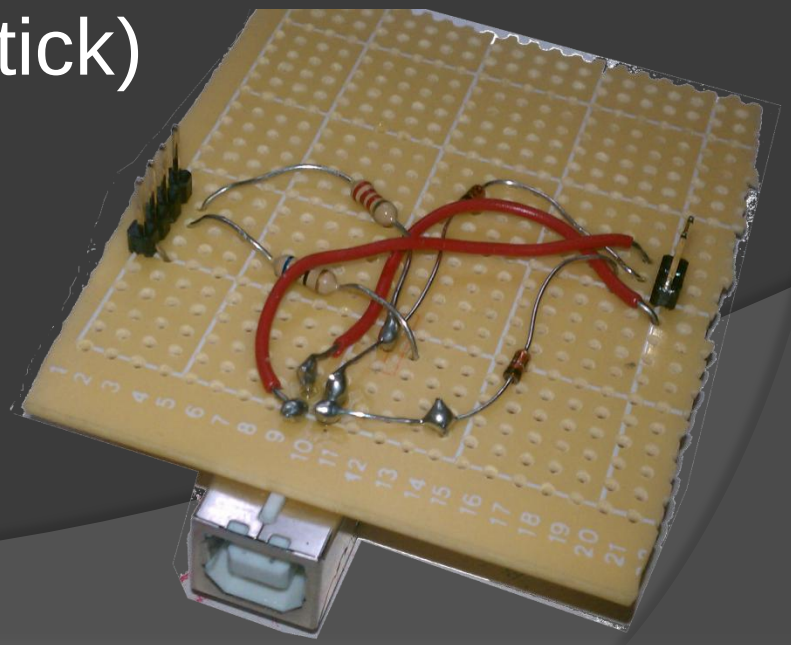


Image Source: Instructables “Another Lazer Tripwire”

USB HID emulator

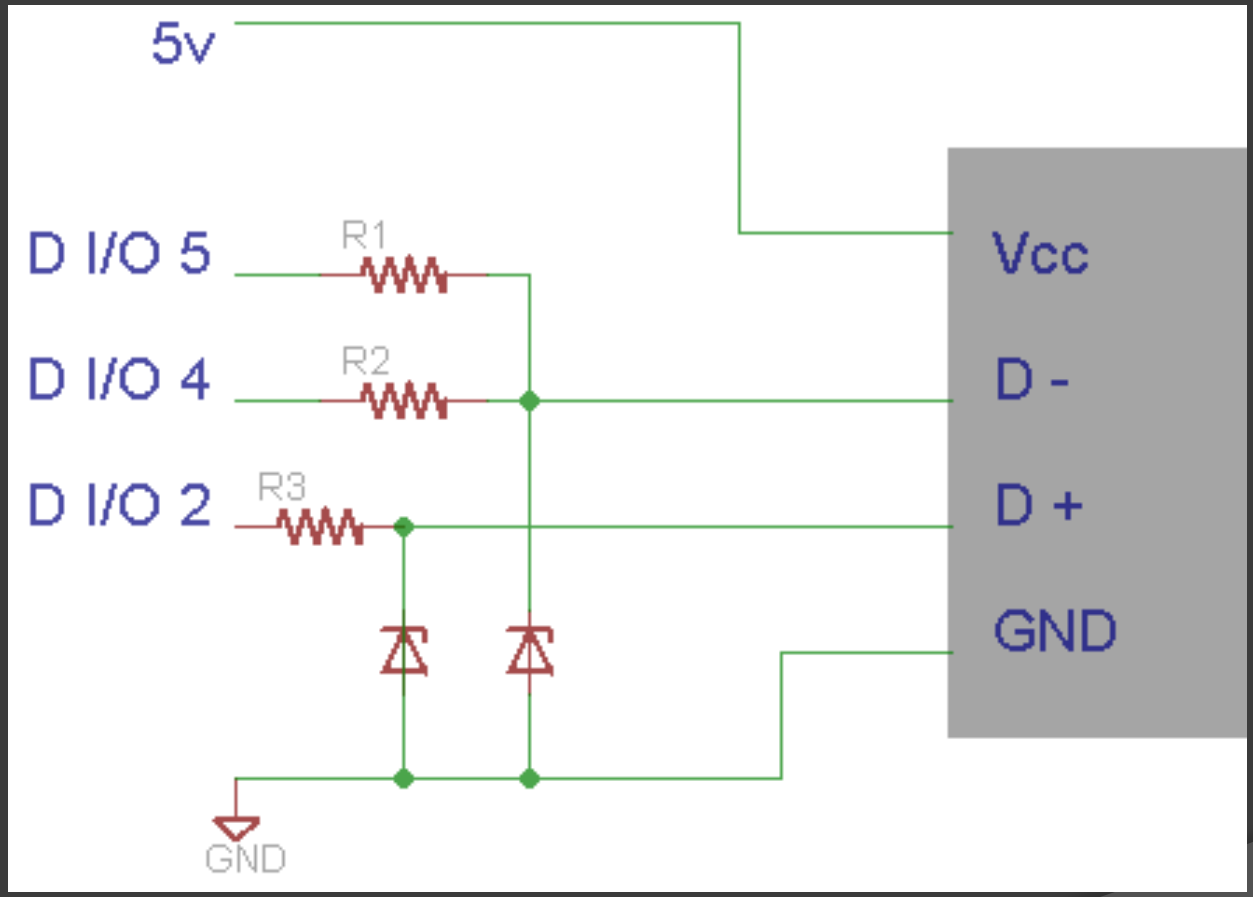
- Based on the AVR project V-USB
- simple circuit, 3 resistors and 2 diodes
- Detected as a keyboard (no drivers)
- can be modified to emulate other USB devices (mouse, joystick)



Security Uses

- Break out of a kiosk mode by trying every possible combination of keys.
- connect it to a computer while the user is away, then after they come back and log in you could distract the user and have it issue commands while the user isn't paying attention (i.e. commands to create a user).
- See Adrian Crenshaw and Follower's talk for more

Schematic



Code

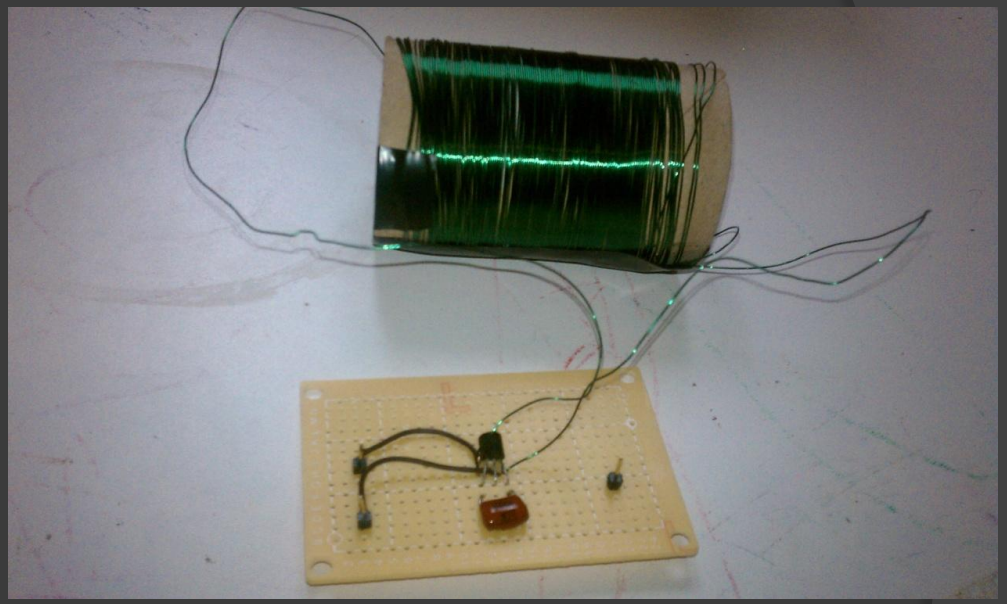
```
//clear built in timers
TIMSK0&=!(1<<TOIE0);
cli();

//connect to computer
usbDeviceConnect();

//send keystrokes
UsbKeyboard.sendKeyStroke(KEY_A);
UsbKeyboard.sendKeyStroke(KEY_B);
```

RFID Emulator

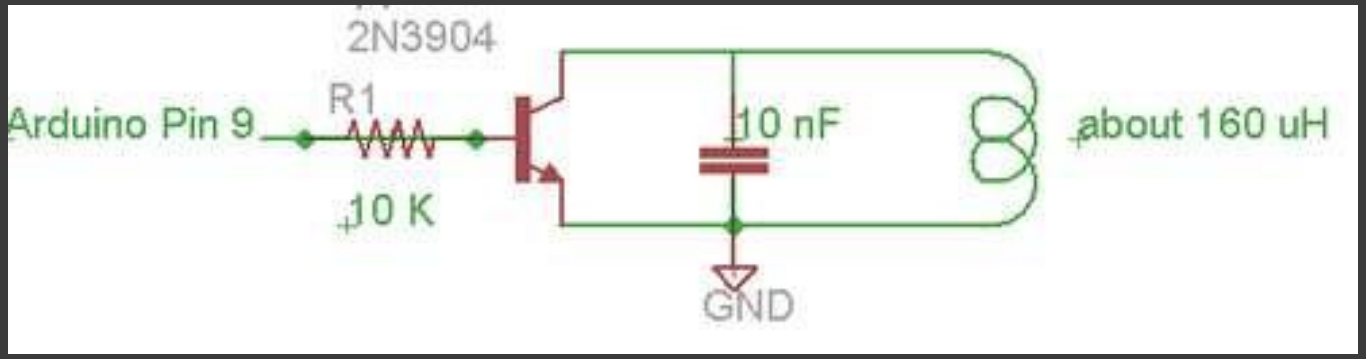
- Goal: make a working 125 KHz emulator
- No oscilloscope or antenna tuning equipment
- No plans to go off (some similar projects though)

RFID Tag Spoofer–Stupid Simple

- Parts
  - 10 K Ohm resistor
  - Transistor
  - 10 nF capacitor
  - Spool of wire from Radio Shack
  - Spent toilet paper roll
- The code is about 20 lines long



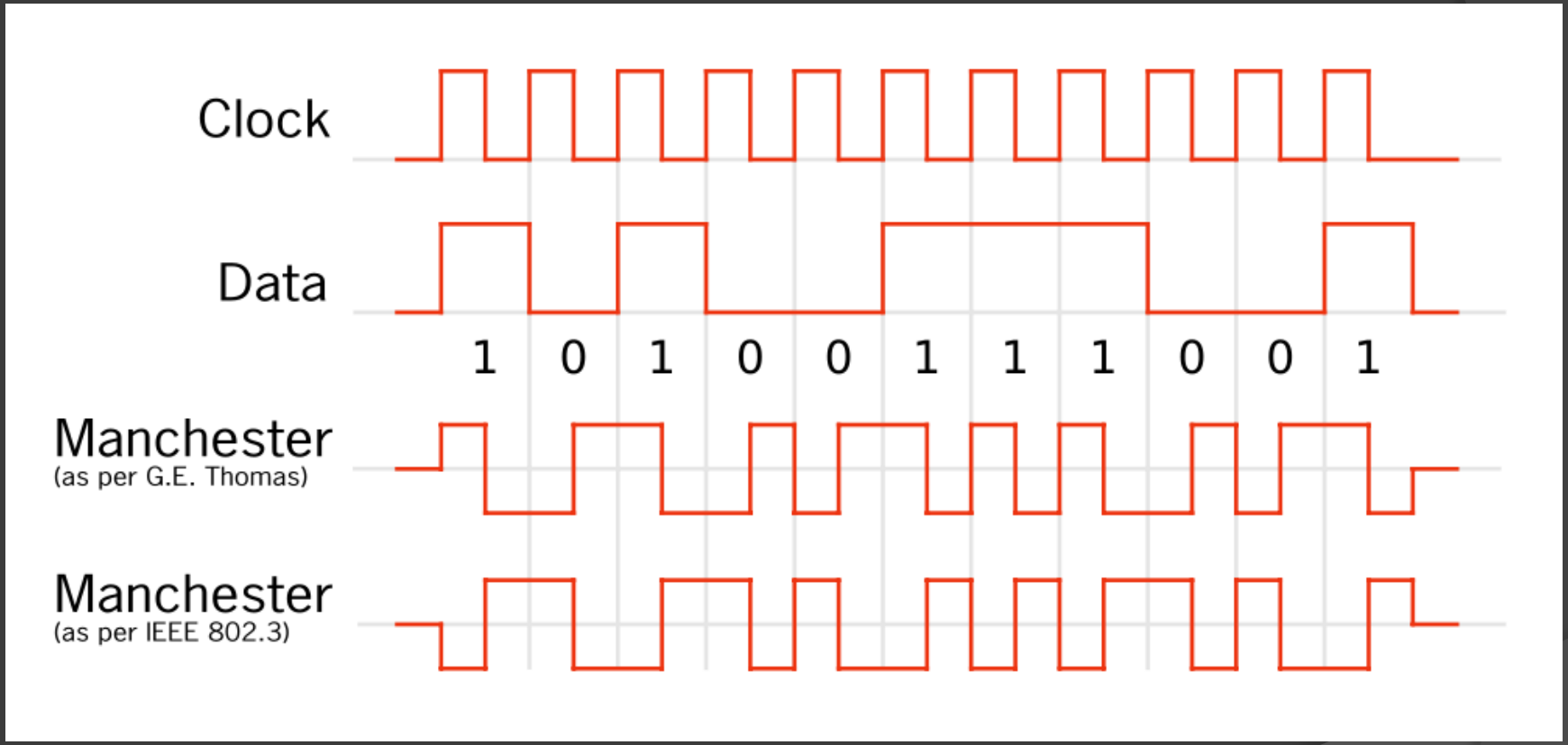
Schematic



Setup

```
#define coil_pin  9;

void setup()
{
  //Set pin as output
  pinMode(coil_pin, OUTPUT);

  //Start it as low
  digitalWrite(coil_pin, LOW);
}
```

Manchester Encoding



*Source Wikipedia Manchester Code

Main Loop Code

```
void loop() {
  //this is the card data we're spoofing.  It's basically 10 hex F's
  int data_to_spoof[64] = {1,1,1,1,1,1,1,1,1,1, 1,1,1,1,0 ,1,1,1,1,0,
    1,1,1,1,0 ,1,1,1,1,0, 1,1,1,1,0 ,1,1,1,1,0, 1,1,1,1,0 ,1,1,1,1,0,
    1,1,1,1,0 ,1,1,1,1,0, 0,0,0,0,0};
  for(int i = 0; i < 64; i++)   {
    set_pin_manchester(0, data_to_spoof[i]);
    delayMicroseconds(256);
    set_pin_manchester(1, data_to_spoof[i]);
    delayMicroseconds(256);
  }
}
```

Manchester Code

```
void set_pin_manchester(int clock, int signal) {
  int man_encoded = clock ^ signal;
  if(man_encoded == 1)   {
     digitalWrite(coil_pin, LOW);
  }
  else  {
    digitalWrite(coil_pin, HIGH);
  }
}
```

Serial

- Arduino digital I/O pins 0 and 1 are hardware serial pins
- Other digital I/O pins can be software serial pins
- Example devices:
  - Parallax RFID Reader
  - GPS Units
  - LCDs
  - Various Integrated Circuits

I2C

- Analog pins 4 and 5 are I2C pins
- I2C is a bus
  - Can connect up to 128 devices
  - Each device has it’s own address
- Examples:
  - Centipede Shield
  - Wii Nunchuck
  - LCDs

Reverse Engineering Hardware using I2C and Serial

- Arduino can be connected to other devices that support I2C and/or Serial to try and determine how they work.
- Examples:
  - Connecting to serial pin on a Seagate hard drive
  - Connect to I2C bus of a Wii Controller
  - I2C Scanner

Parallax RFID Reader

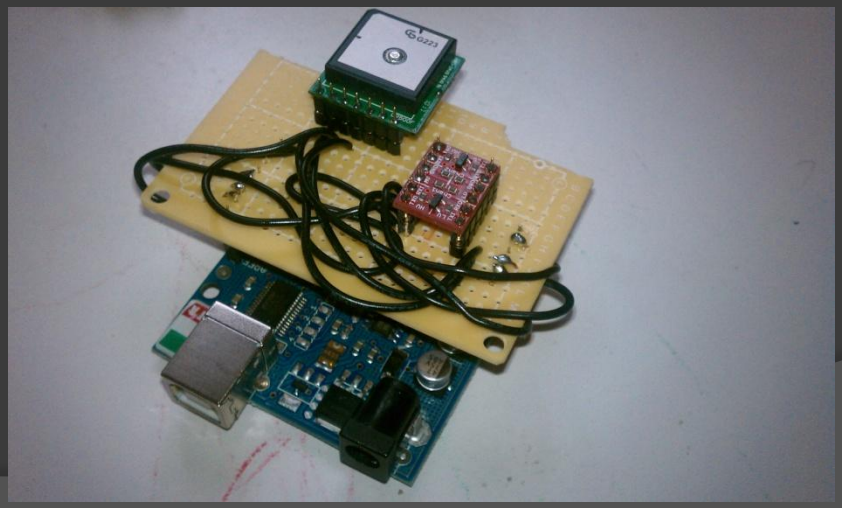
- Serial device
- 2400 Baud

Code

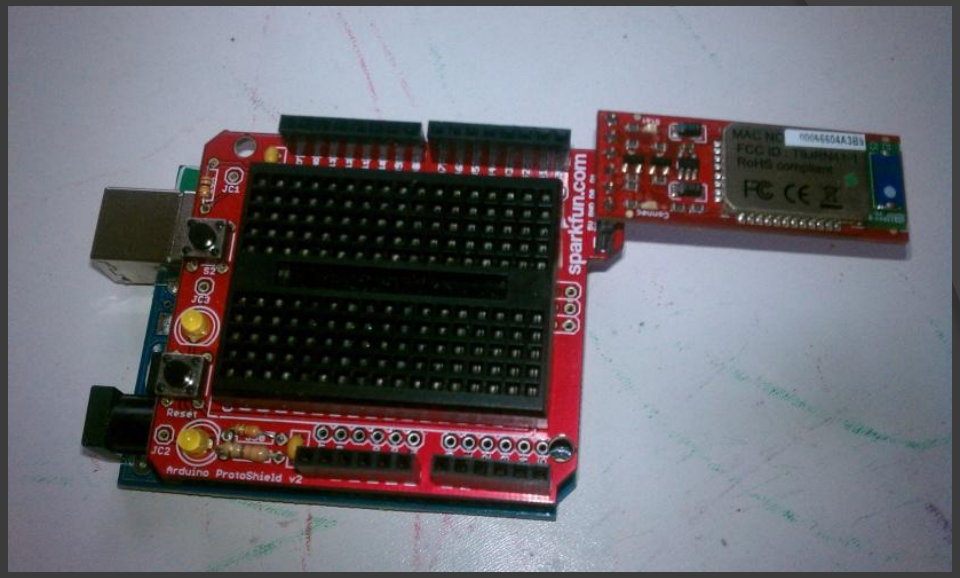
```
#include <NewSoftSerial.h>

NewSoftSerial mySerial(6, 7);

void setup()  {
   mySerial.begin(2400);
   Serial.begin(9600);
}

void loop()  {
  if (mySerial.available()) {
      Serial.print((char)mySerial.read());
  }
}
```

GPS Tracking Device

- Uses a serial GPS unit
- Can log data to an SD card or broadcast it (i.e. Xbee, bluetooth or cellular).
- Used to track down stolen good
- Used to see where people are



Bluesmirf



- Serial Device
- Coverts Bluetooth Serial (SSP) to TTL
- Default Baud Rate 115200, can be changed
- Can be used to program an Arduino
- Can be used to communicate with other bluetooth devices

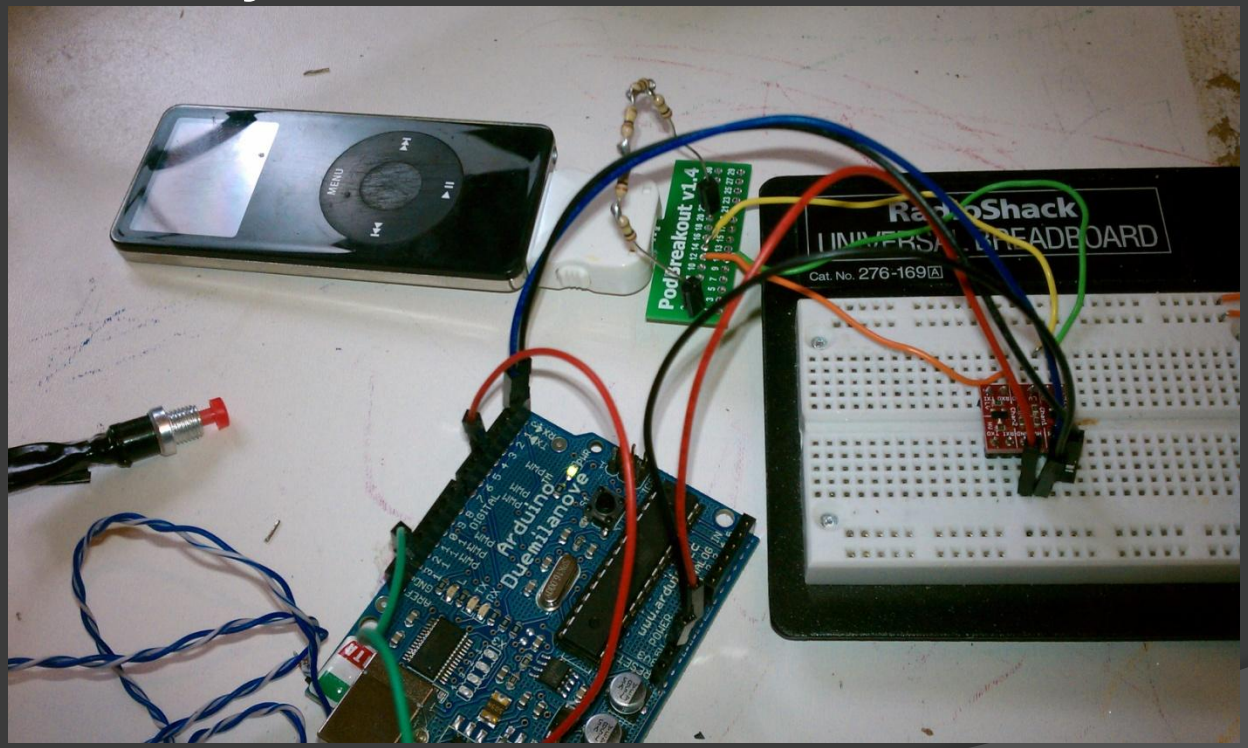
Bad Bluesmirf

Arduino Meets Android

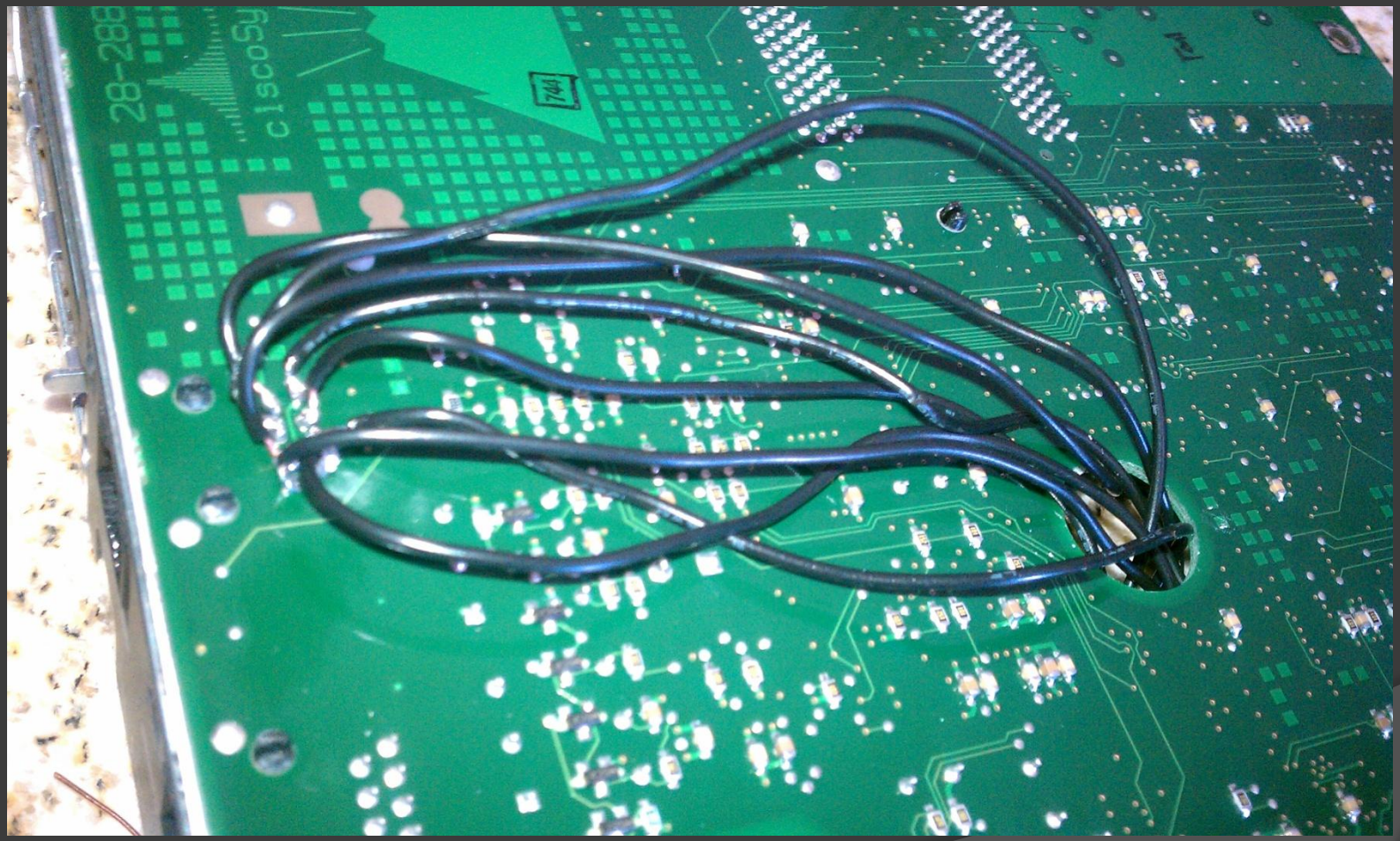
- Amarino Project
- Phone can control Arduino
- Arduino can Control Phone

PodBreakout

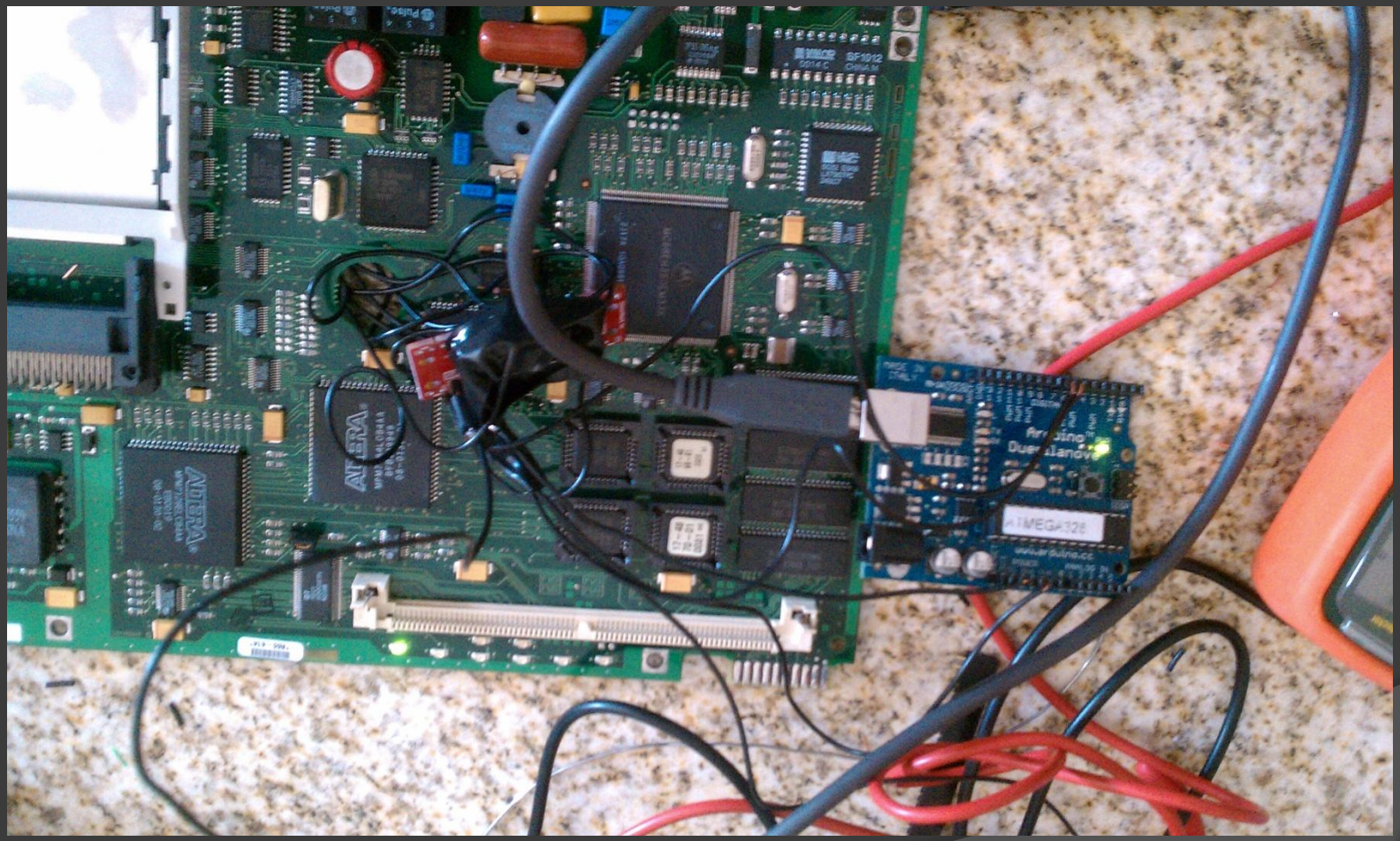
- Connects to an iPod or iPhone
- Ability to send serial commands



Inside Cisco Router

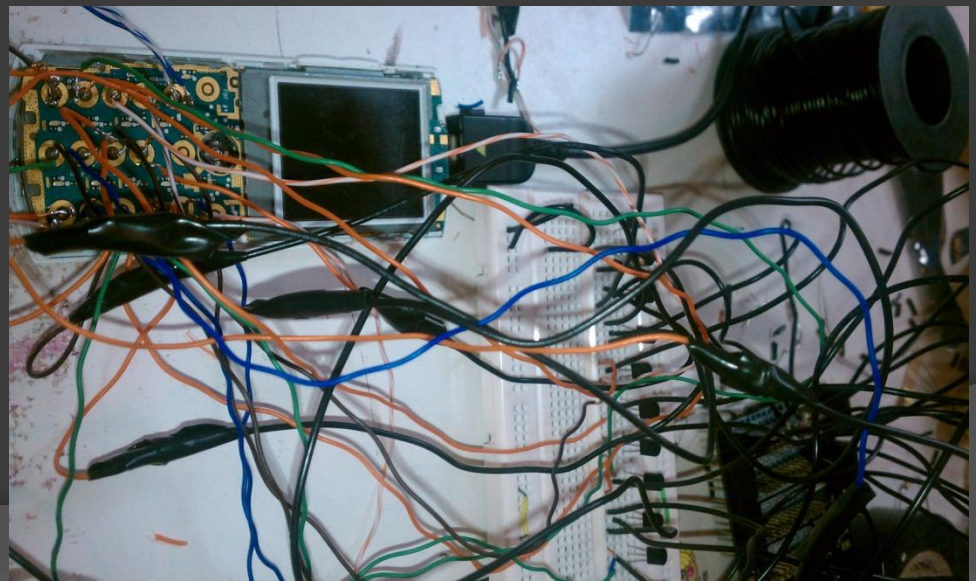


Inside Cisco Router



Integrate with Cellphone

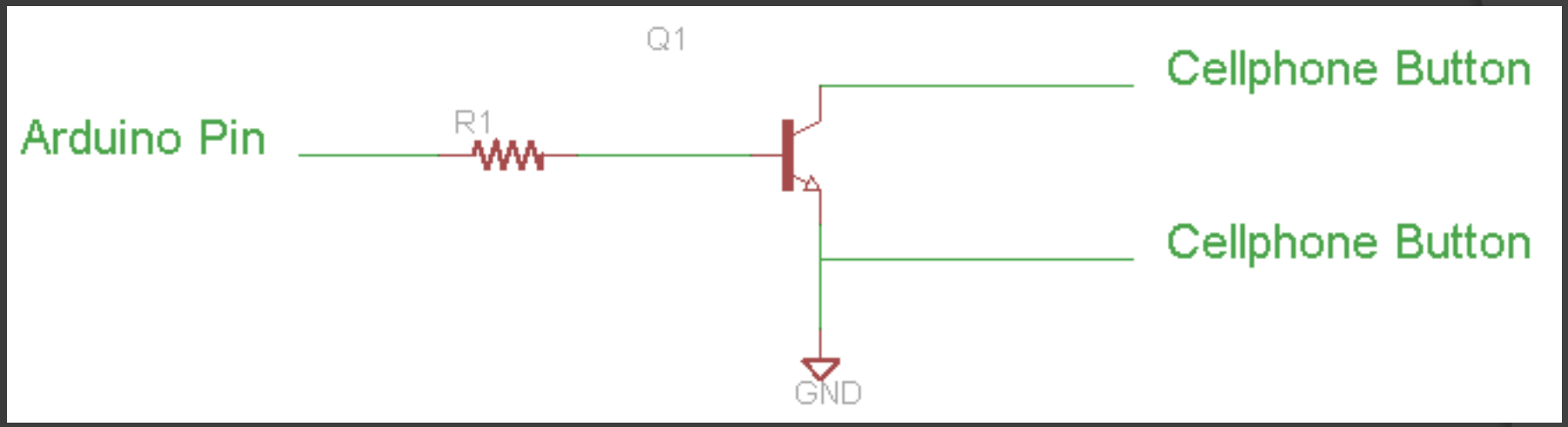
- Solder transistors to the keypad of a cheap prepaid cell phone
- connect the transistors to the Arduino
  - Alternative is to use a shift register
  - I used a centipede shield



Uses

- Communication to remote devices
- Interact with touch tone systems

Schematic

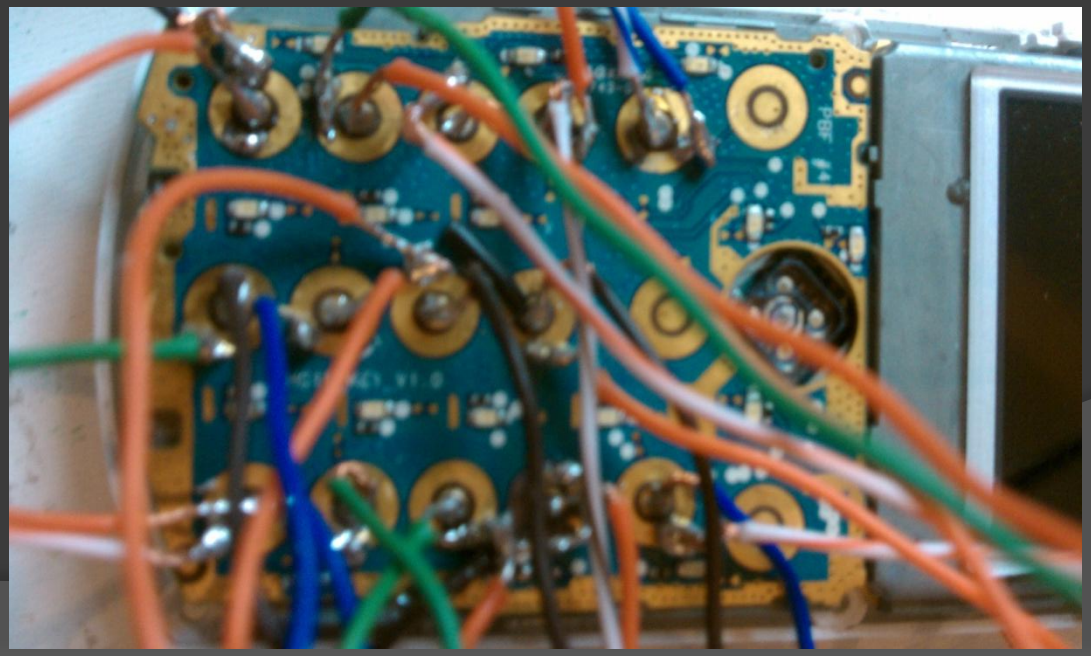


Video

- That’s all, just play the video!

Other Uses for this Technique

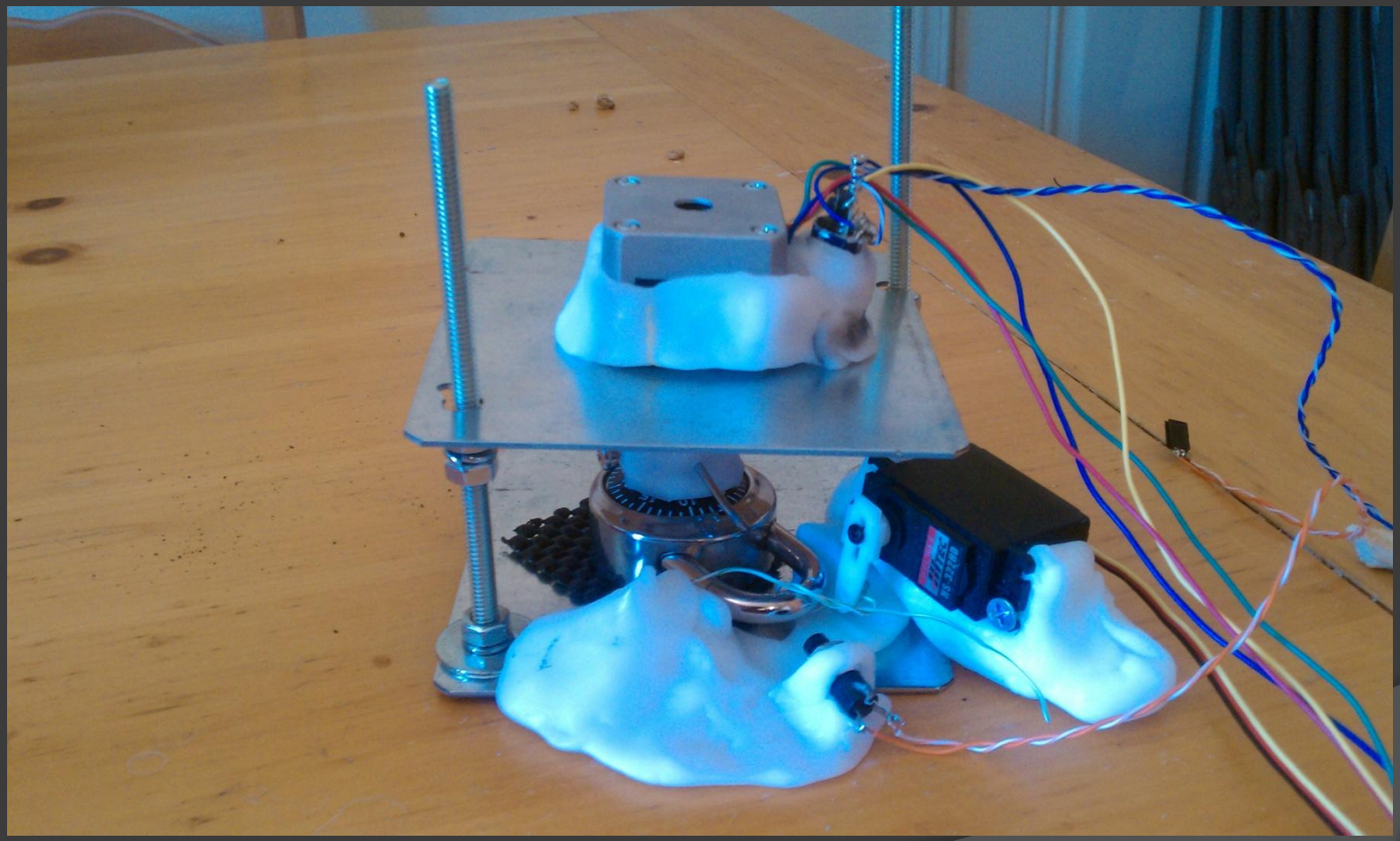
- You can use this technique for almost anything you want to automate button pushes on (and you don't mind soldering to the device).



Combination Lock brute forcer

- Stepper motor turns the dial
- Servo tries to open the lock
- A laser pointing to a photoresistor, detects 0
- Tries every possible combination
- Can use known algorithms (i.e. stop numbers for Master Locks)

Combination Lock Brute Forcer

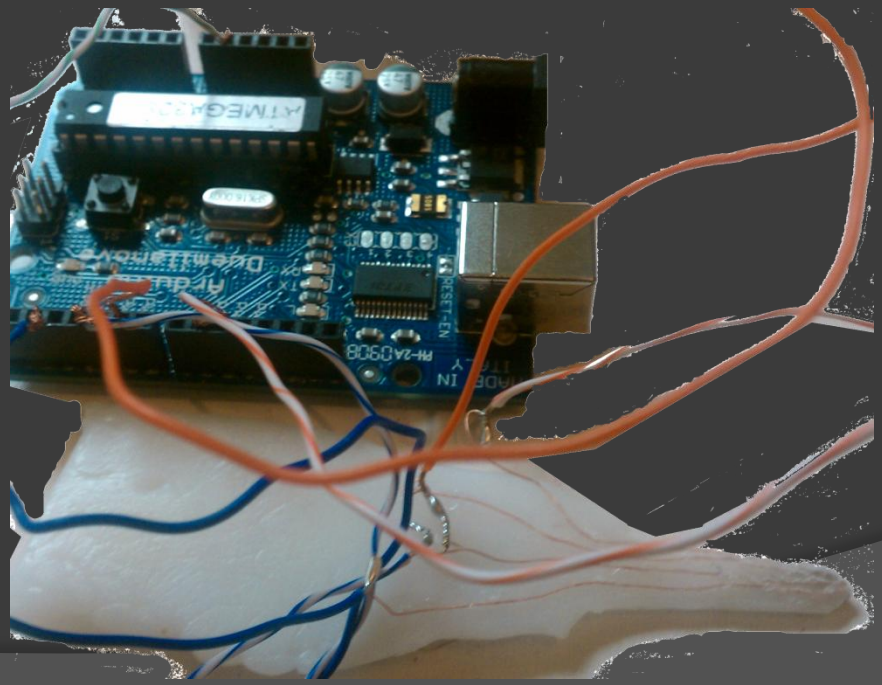


ShapeLock is Rad

- Plastic beads the melt in water heated in the microwave
- You can make it into whatever shape you want
- When it cools you can cut it, drill it, etc.

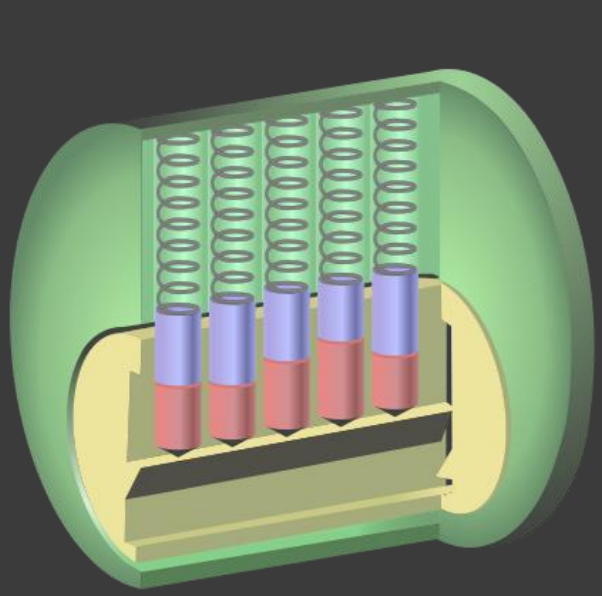
Key Impressioner

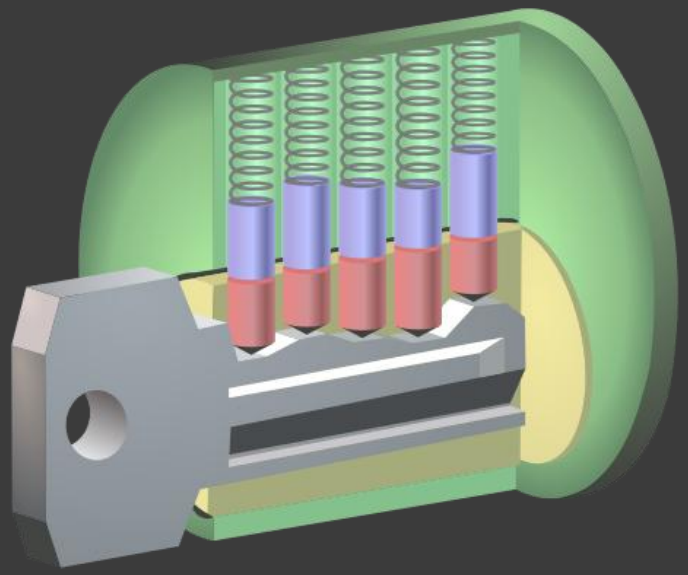
- Works on wafer locks
- Several exposed pieces of wire
- Wire connected to the body of the lock



Wafer vs Pin Locks

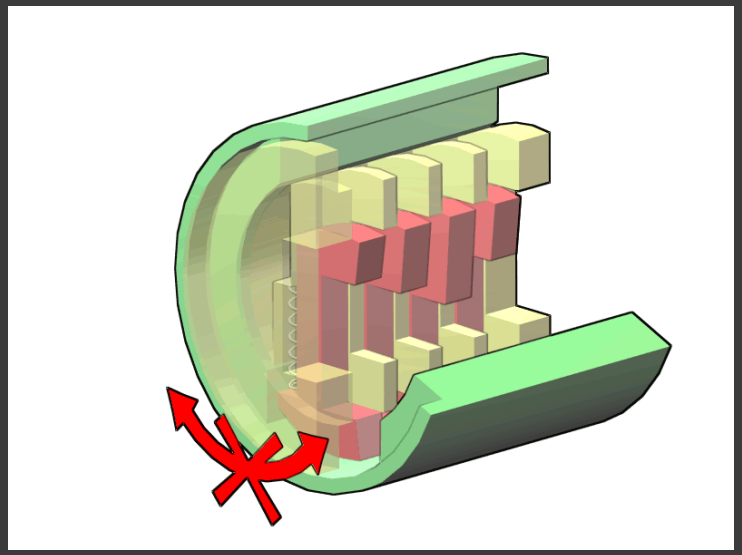
- Pin Tumbler Locks

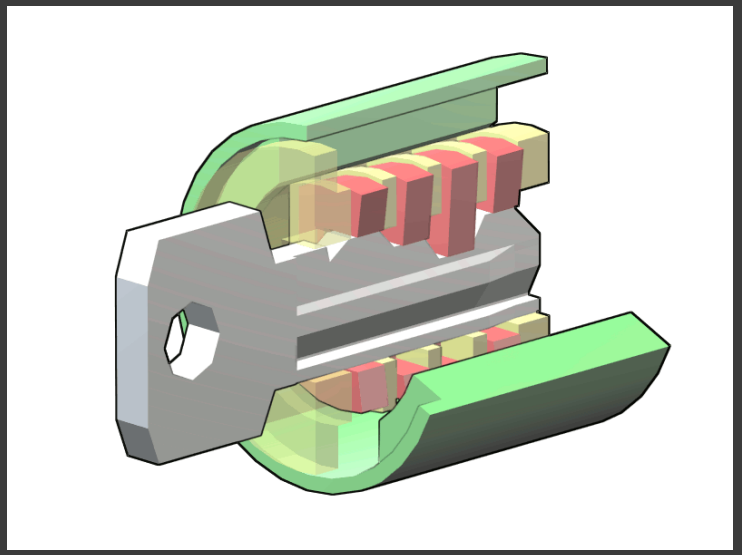




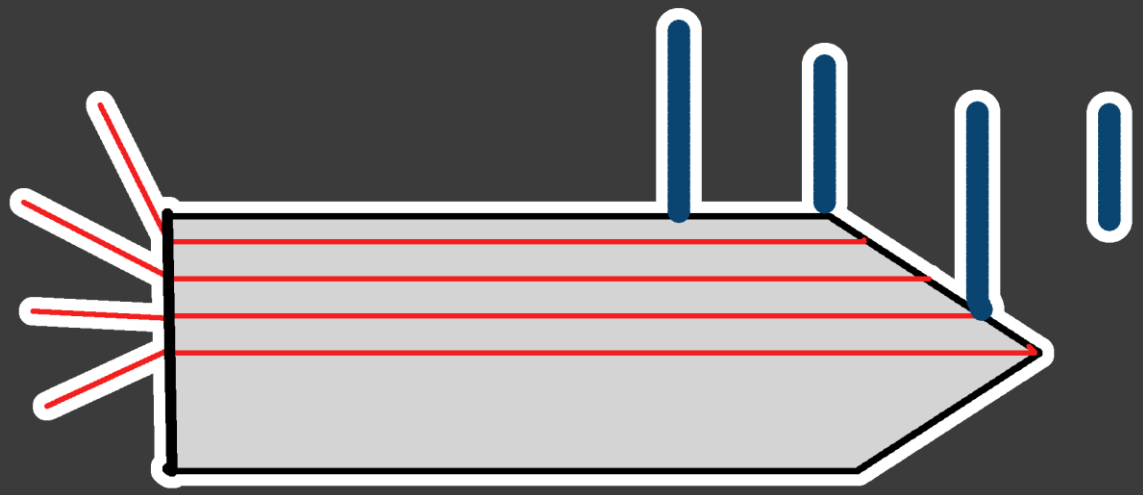
Wafer vs Pin Locks

- Wafer Tumbler Lock





Key Impressioner



Combining devices

- The real power comes in combining several devices.
- Examples
  - Xbee and Ethernet Shield
  - RFID reader that broadcasts what it reads using an Xbee
  - Bluetooth and motor control

Other Interesting Projects

- crypto-arduino-library
- Unlock doors by knocking
- Identify a person by handshake
- Arduino based oscilloscope

Alternatives

- Parallax Propeller
  - Has 8 cogs for parallel computing
- AVR (no Arduino stuff)
  - cheap, code directly in C
- Microchip PIC
  - cheap, code in C or assembly
- Freescale DSC
  - used on DEFCON badges, CodeWarrior pretty easy to use especially with Processor Expert

Resources

- Arduino.cc
  - The official Arduino website
  - Great forums
- Instructables.com

- Sparkfun.com
- Adafruit.com
- Makershed.com
- Evilmadscientist.com
- Seeedstudio.com
- Pololu

- Google!

Where to Go to Learn More

- See if you have a local hackerspace
  - Many do Arduino projects
  - If there isn't one, start one
- Local Make Groups
  - Same as above
- Come to the Hardware Hacking Village

Code and Project Details

- http://github.com/sk3tch/
- @davewking on twitter