Universal RF Usb Keyboard Emulation Device
URFUKED

-by Monta Elkins

monta.defcon @ geekslunch.com

version .08 6/2010

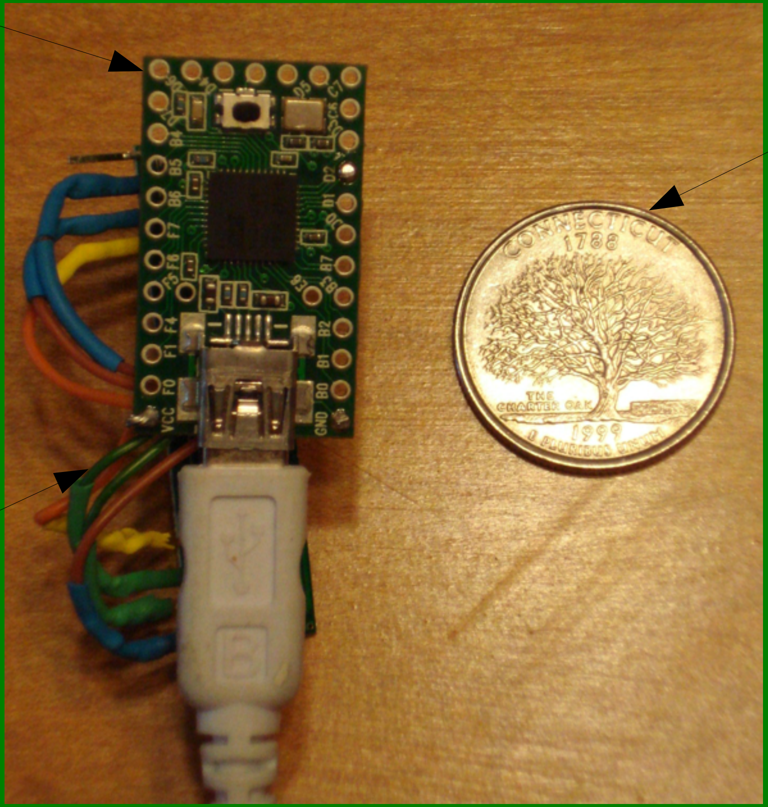
Updates at: http://www.hackerwarrior.com/urfuked

Hardware

Receiver

(plugged into spare USB port)

“Teensy” Microcontroller



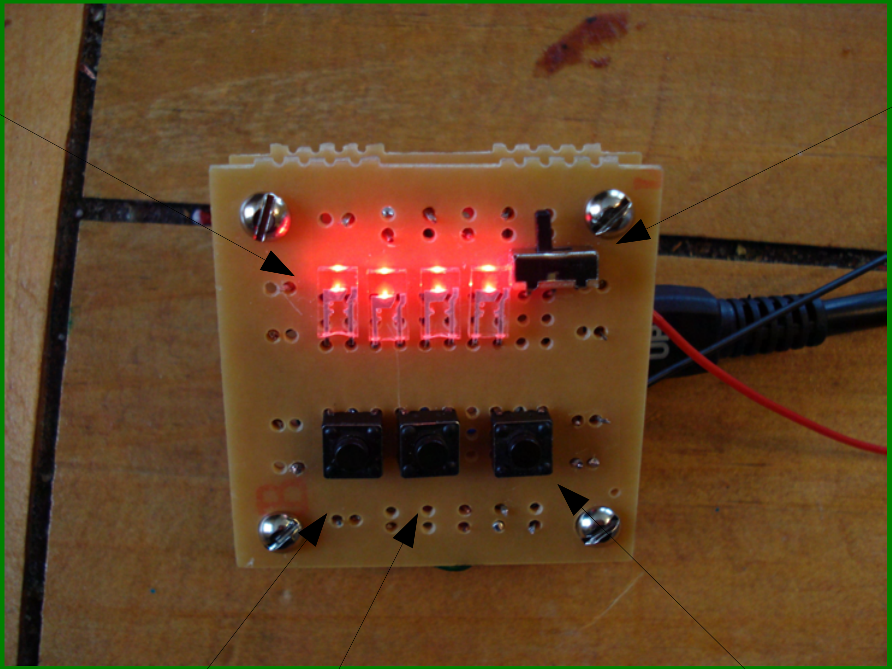
Quarter

RF receiver On the back

- Receiver is very small
- Can be encased in plastic to look like a typical USB key

Pwner

portable, battery powered, rf transmitter



LEDs Show What Attack to Perform

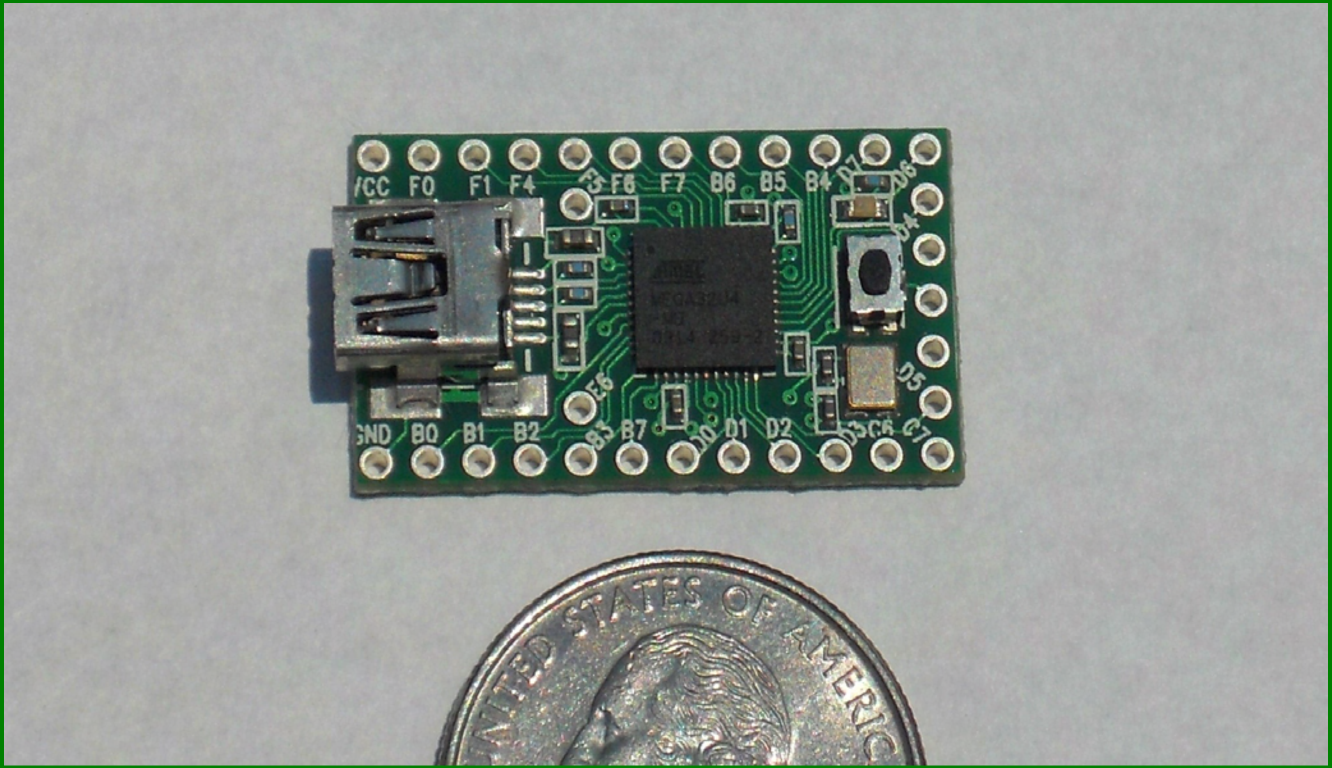
Power Switch

Input Switch Set Attack

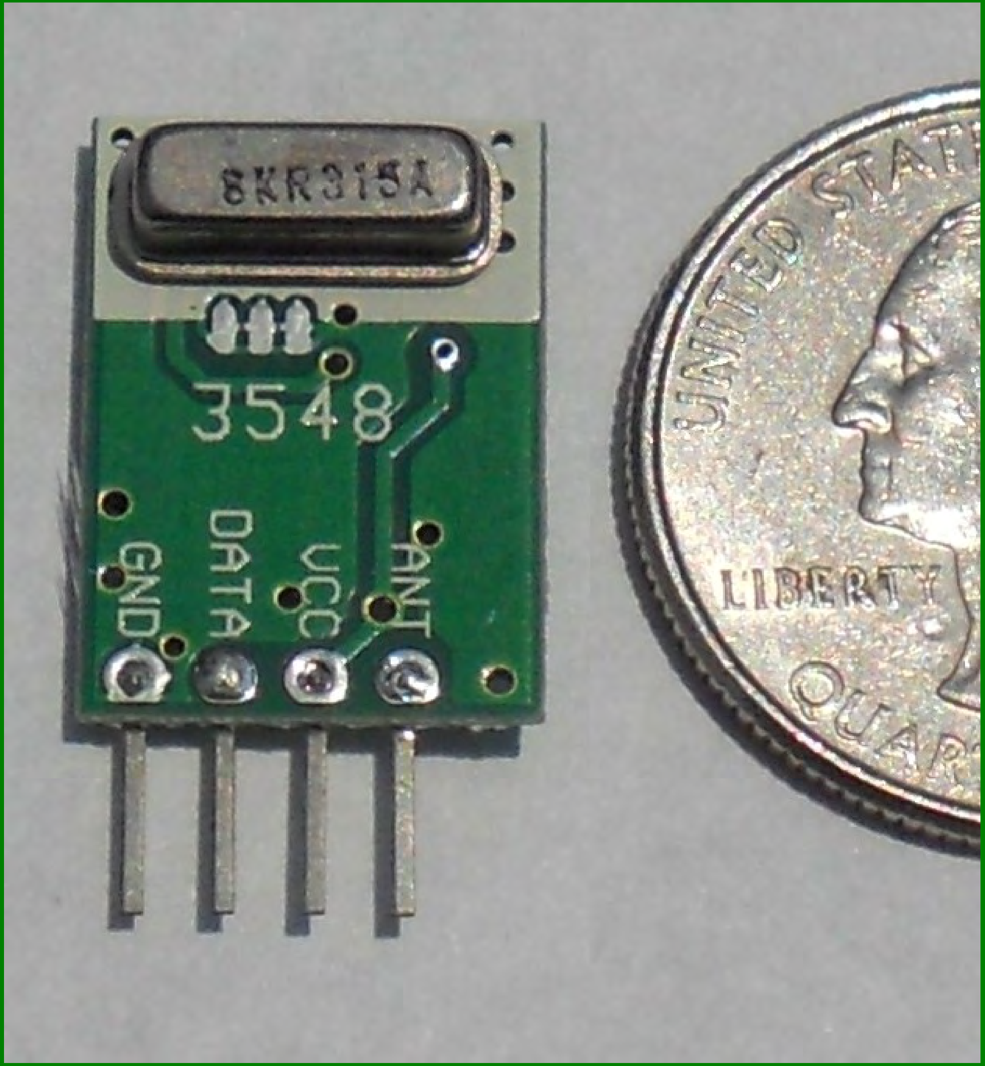
0wnzred Switch Transmits Attack

Hardware Construction

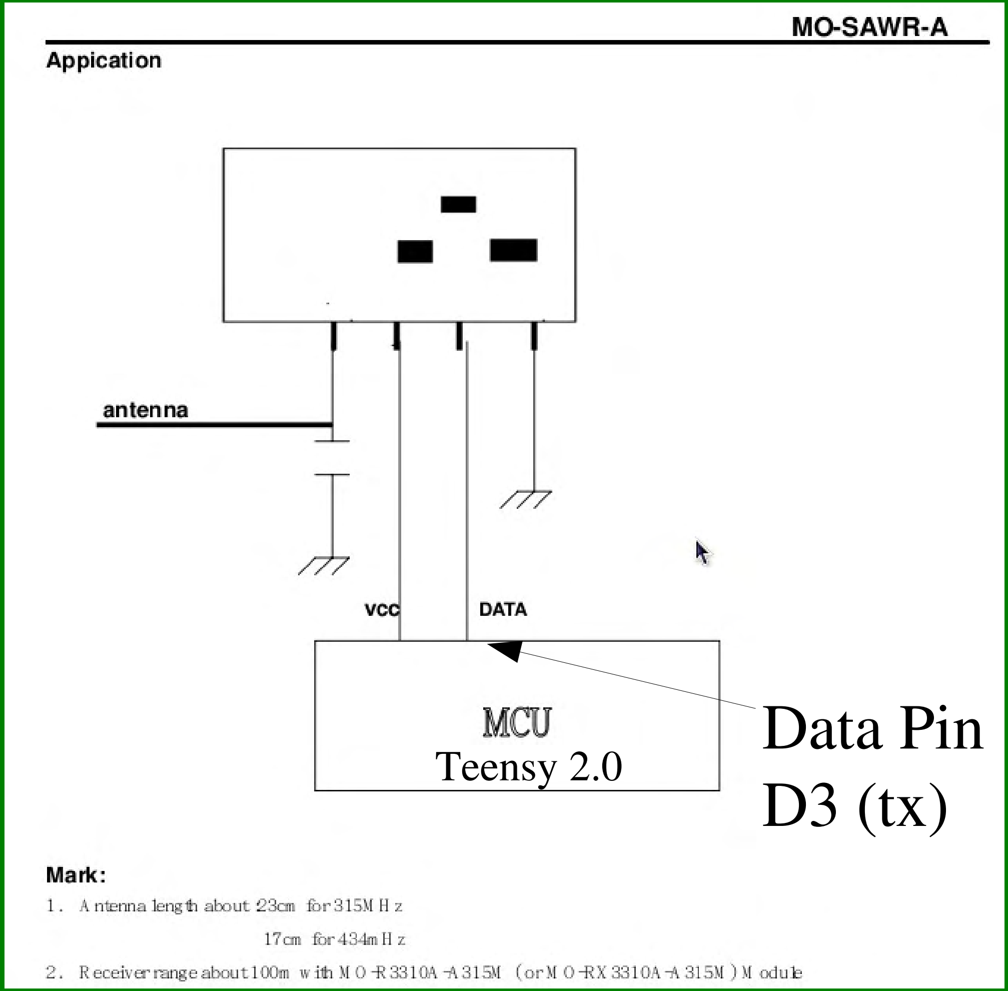
Teensy uc


VCC
F0
F1
F4
F5
F6
F7
B6
B5
B4
D7
D6
D4
E6
D5
GND
B0
B1
B2
B3
B7
D0
D1
D2
D3
C6
C7

Transmitter



Transmitter Datasheet



MO-SAWR-A

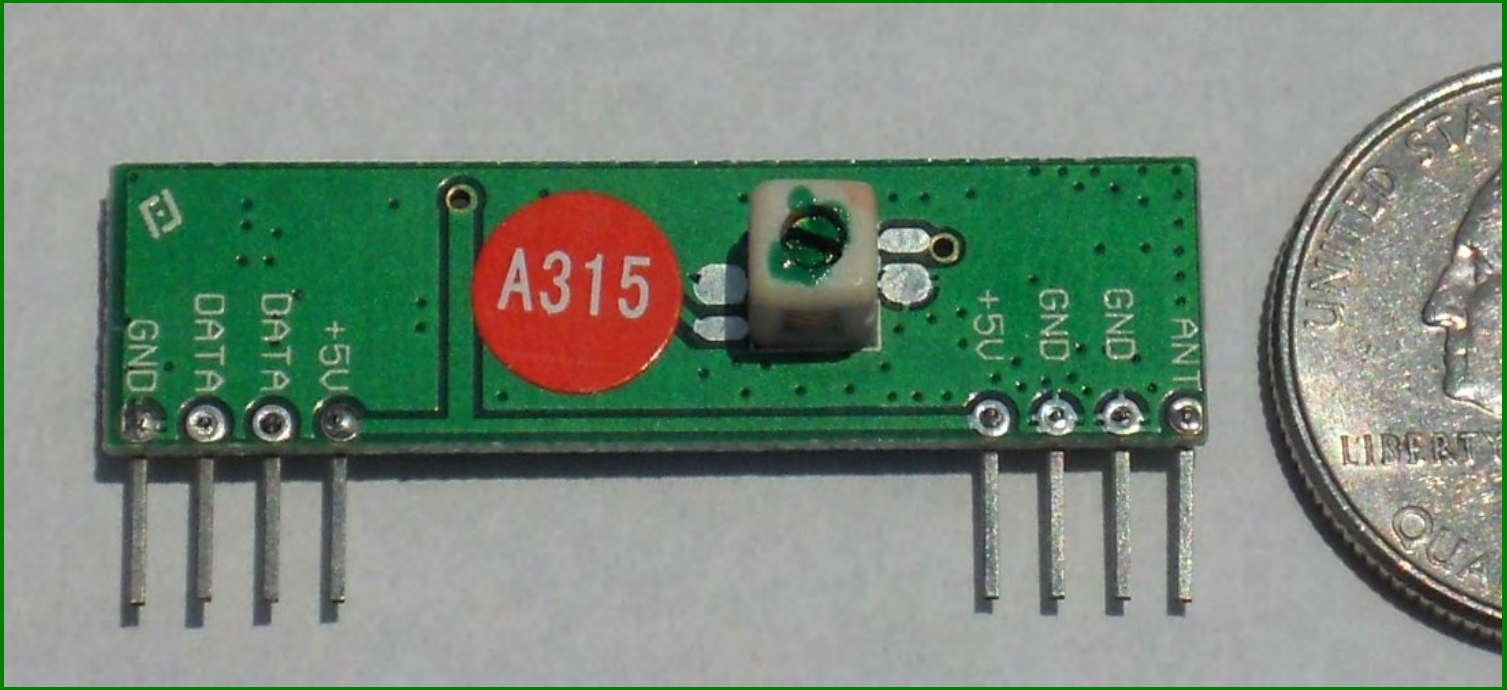
Appication

Mark:

1. Antenna length about 23cm for 315MHz
   17cm for 434mHz
2. Receiver range about 100m with MO-R3310A-A315M (or MO-RX3310A-A315M) Module

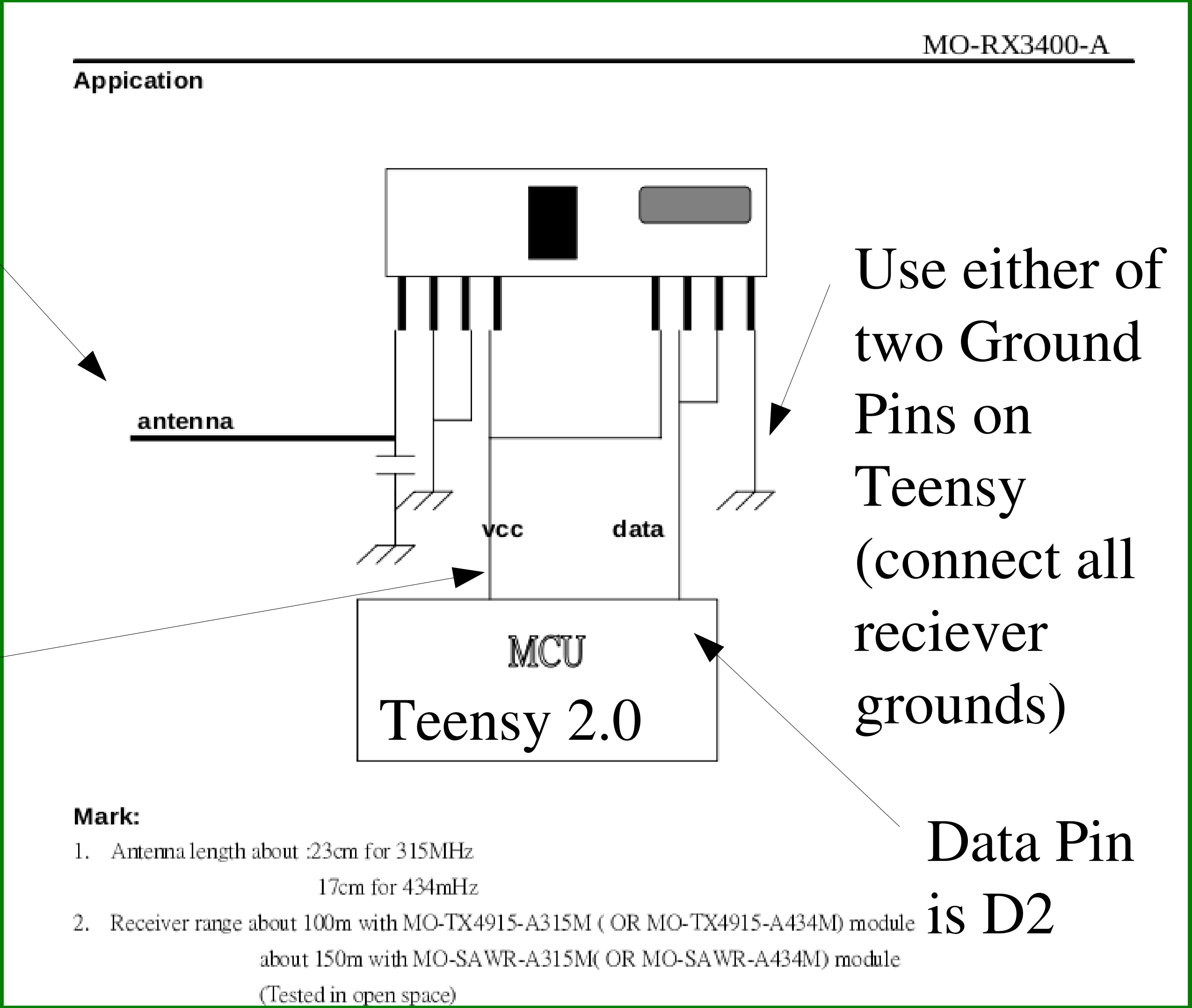
http://www.sparkfun.com/datasheets/Wireless/General/MO-SAWR.pdf

Receiver



Receiver Datasheet

Antenna is 23 cm long



MO-RX3400-A

Appication

Mark:

1. Antenna length about :23cm for 315MHz
   17cm for 434mHz
2. Receiver range about 100m with MO-TX4915-A315M (OR MO-TX4915-A434M) module
   about 150m with MO-SAWR-A315M(OR MO-SAWR-A434M) module
   (Tested in open space)

Use either of two Ground Pins on Teensy (connect all reciever grounds)

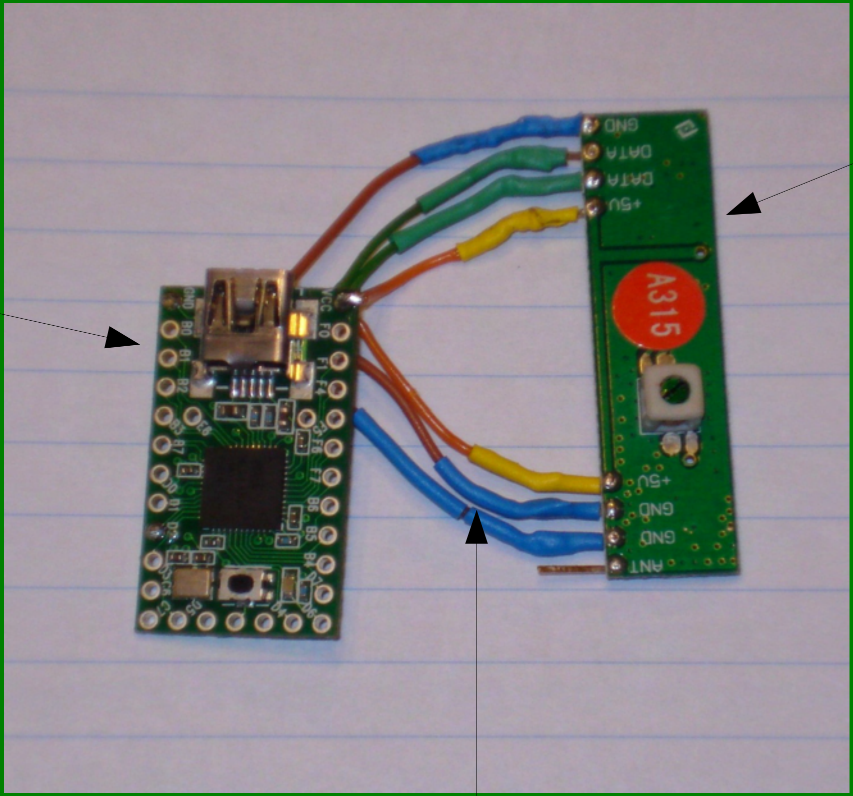
Use either of two Vcc pins on Teensy

Data Pin is D2

http://www.sparkfun.com/datasheets/Wireless/General/MO-RX3400.pdf

Receiver Construction

“Teensy” 2.0
Microcontroller
$18



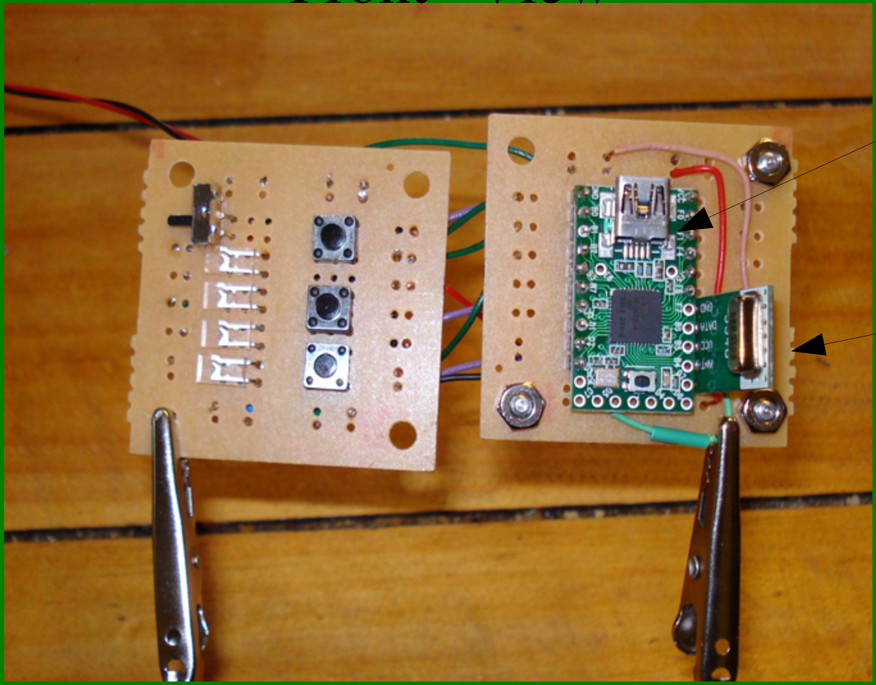
Sparkfun RF
Reciever 315 Mhz
$4.95

Construction consists of soldering 7 wires.
Simple!

Pwner Construction

(rf transmitter)

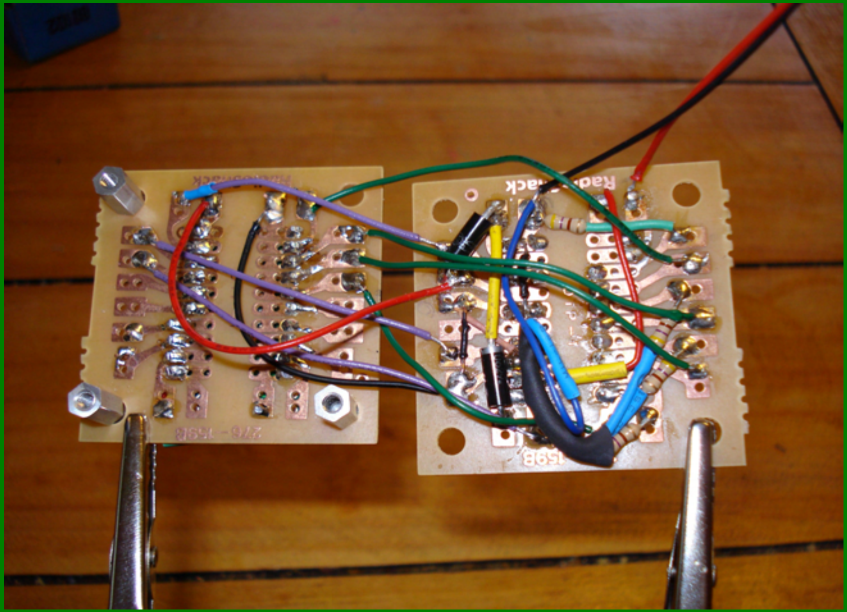
“Front” View



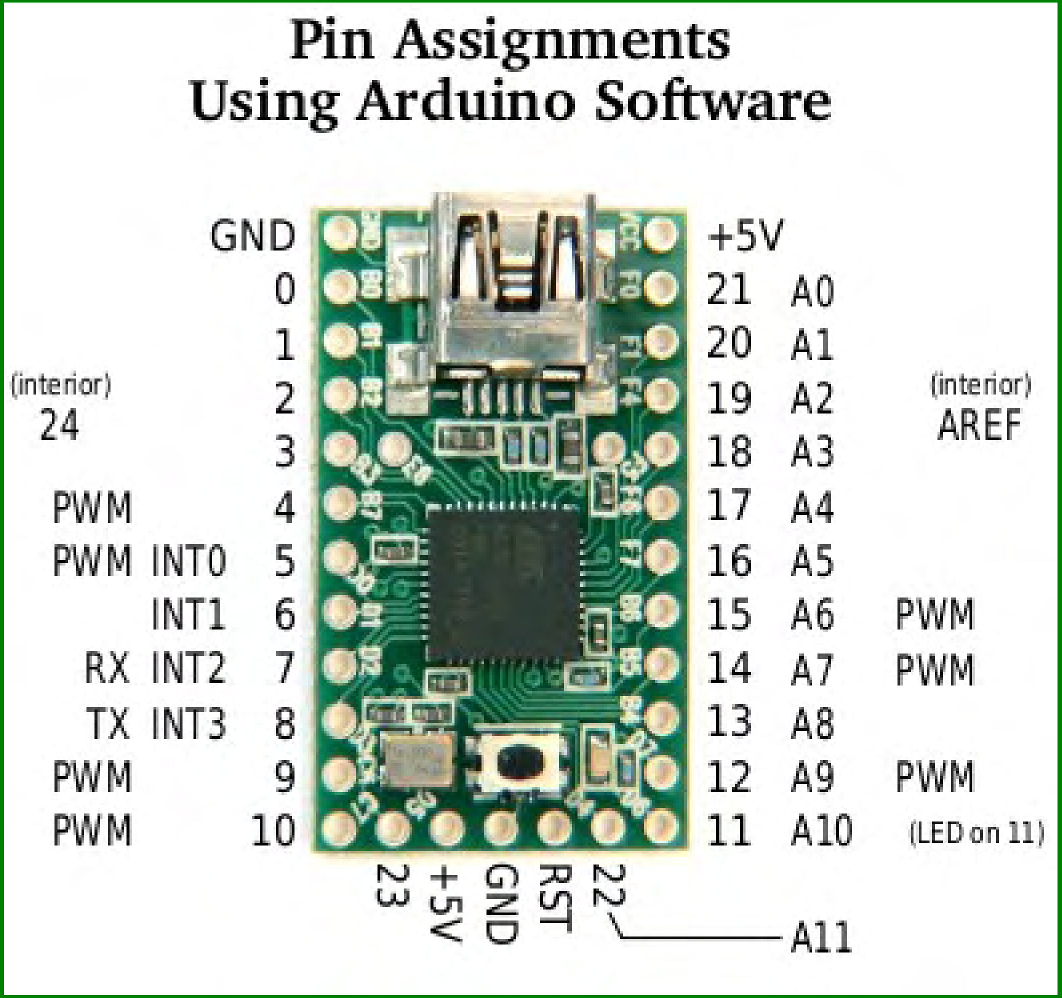
“Teensy” Microcontroller
$18

Sparkfun RF Transmitter
$3.95

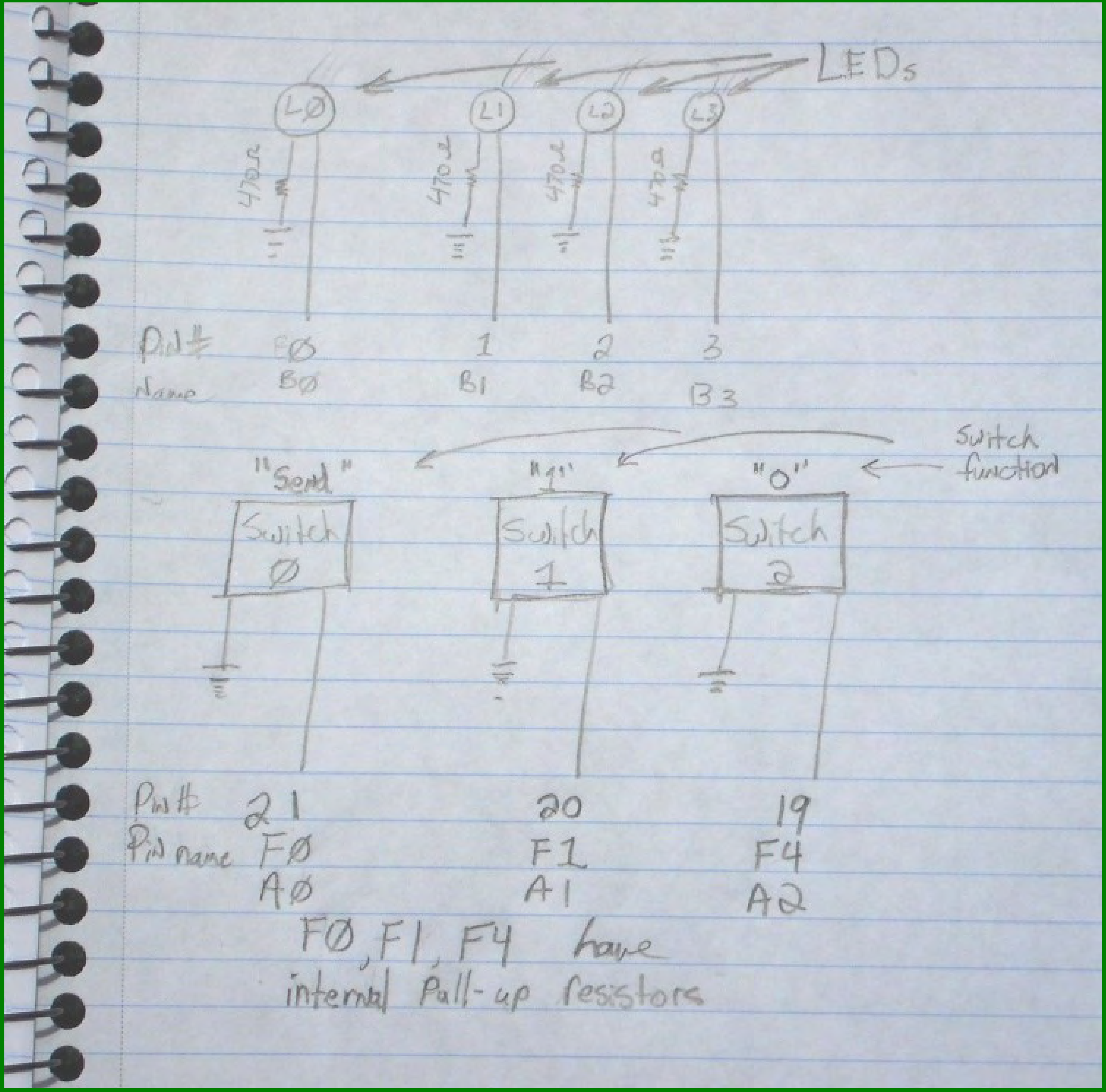
“Rear” View



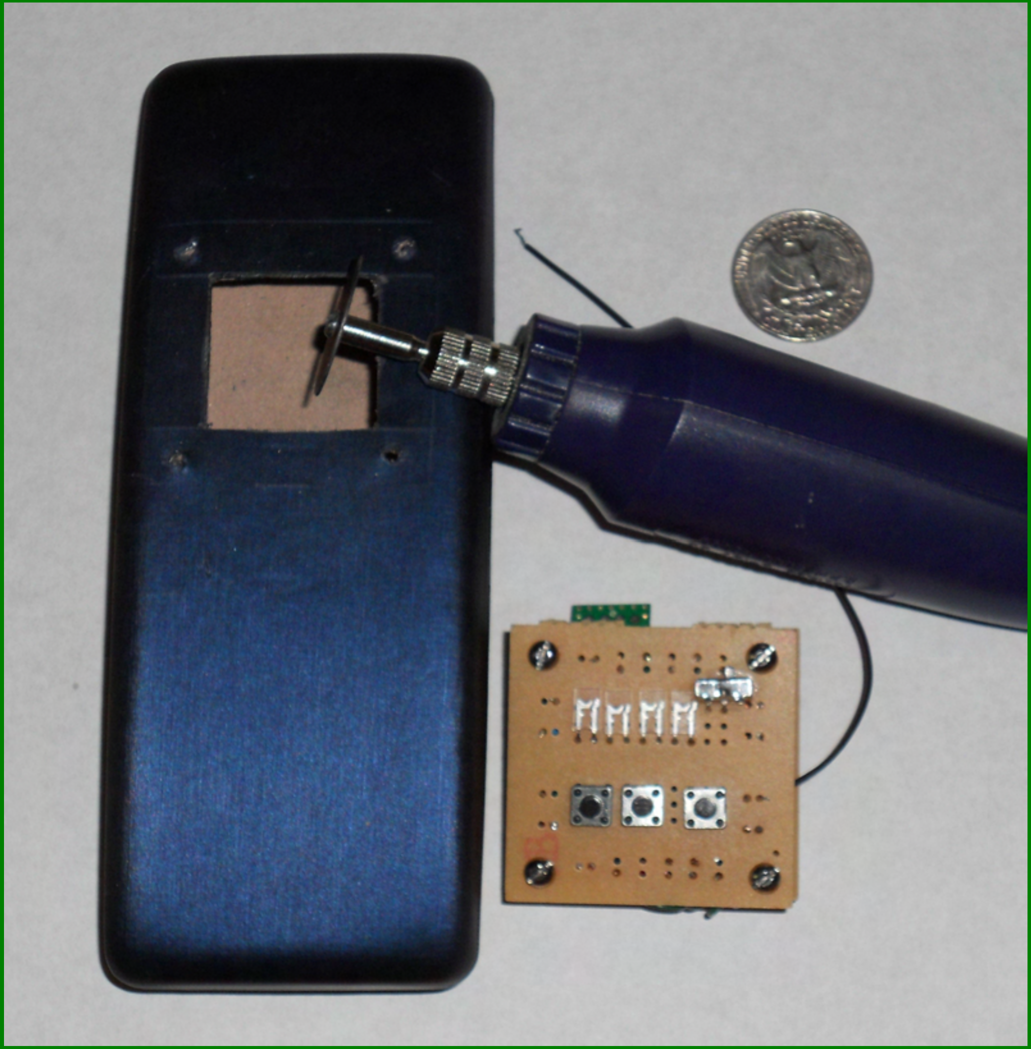
Teensy Pins


Pin Assignments
Using Arduino Software
GND
0
1
(interior)
24
2
3
PWM 4
PWM INT0 5
INT1 6
RX INT2 7
TX INT3 8
PWM 9
PWM 10
23
+5V
GND
RST
22
A11
+5V
21 A0
20 A1
19 A2
(interior)
AREF
18 A3
17 A4
16 A5
15 A6 PWM
14 A7 PWM
13 A8
12 A9 PWM
11 A10 (LED on 11)

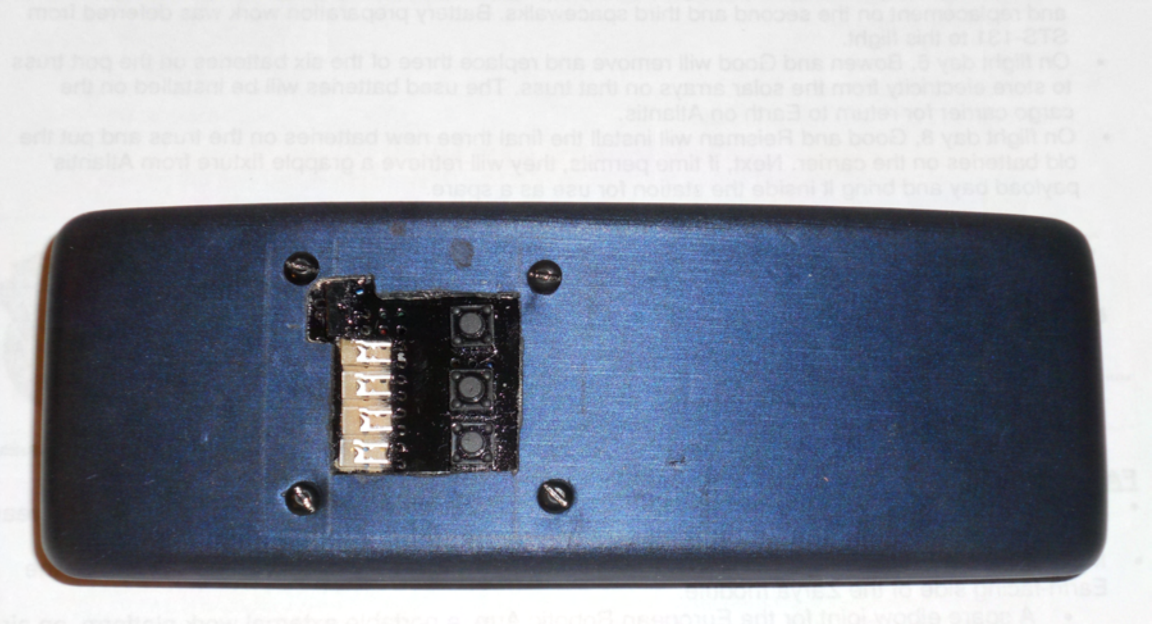
Pwner Schematic

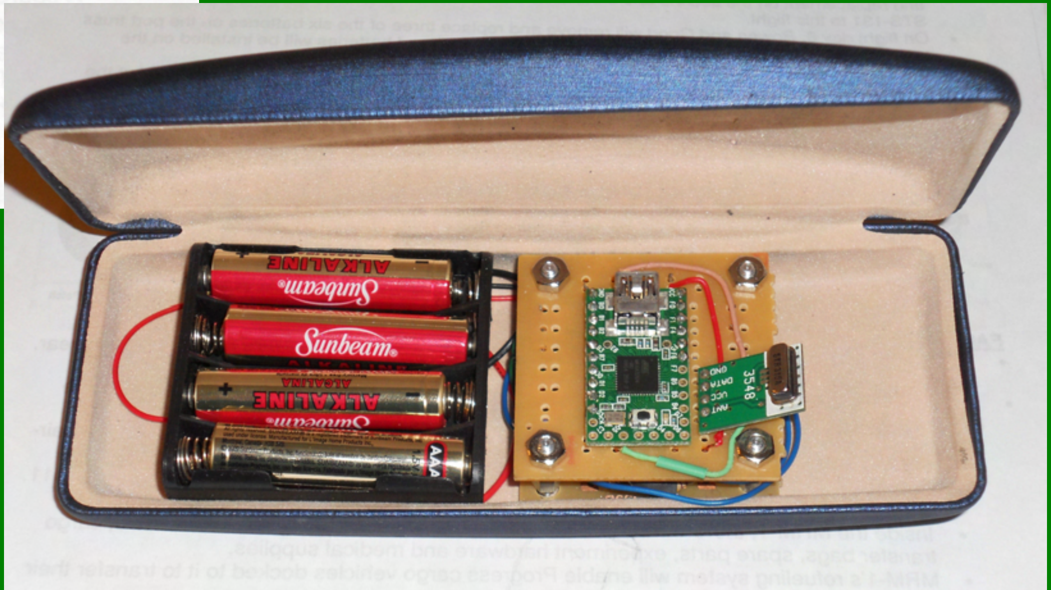


Pwner Case

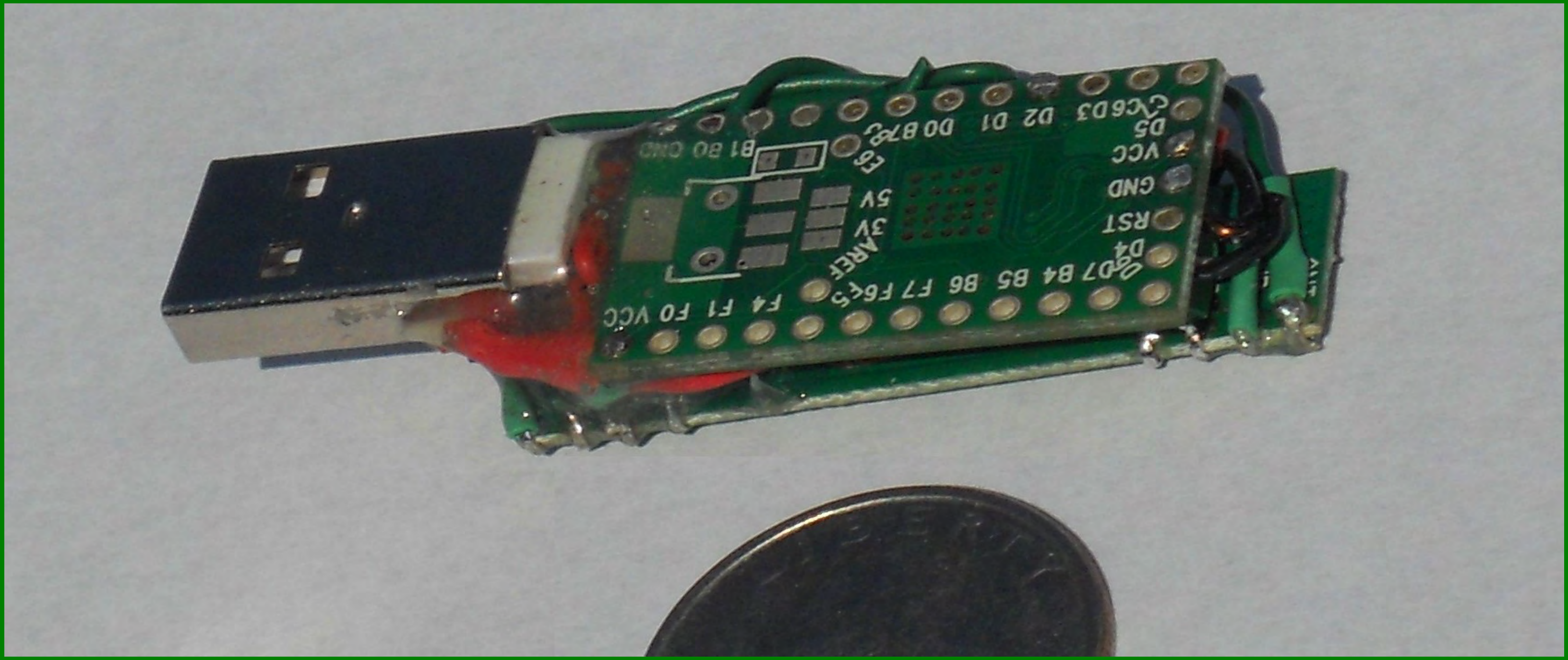


Pwner Case





Receiver Assembled



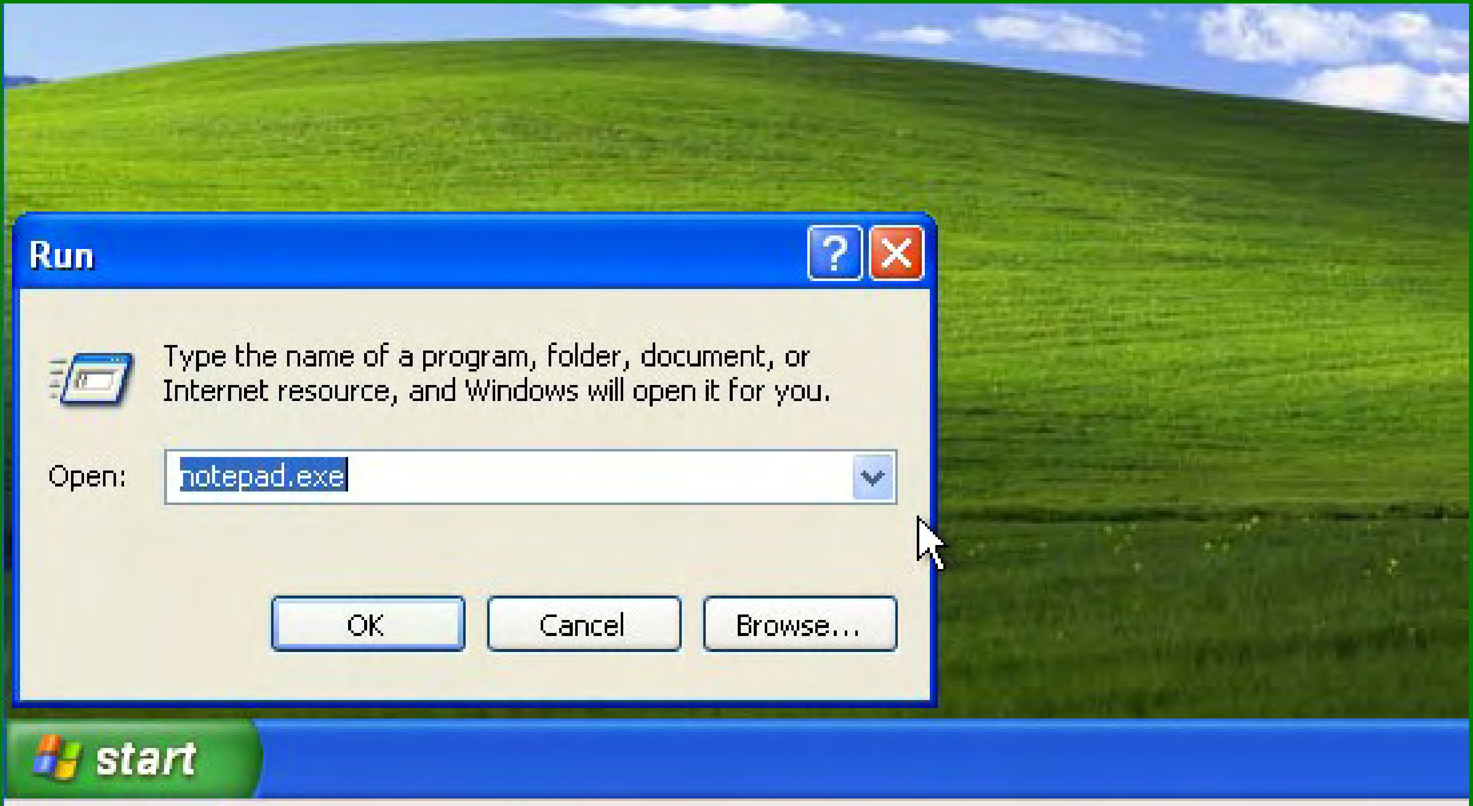
Live Demo

Canned Demo

Windows Attack 01

URFUKED opens the windows run dialog box using the keyboard shortcut "windows key" + R

In this demo it runs the benign command "notepad.exe"- but any other valid command could be executed.

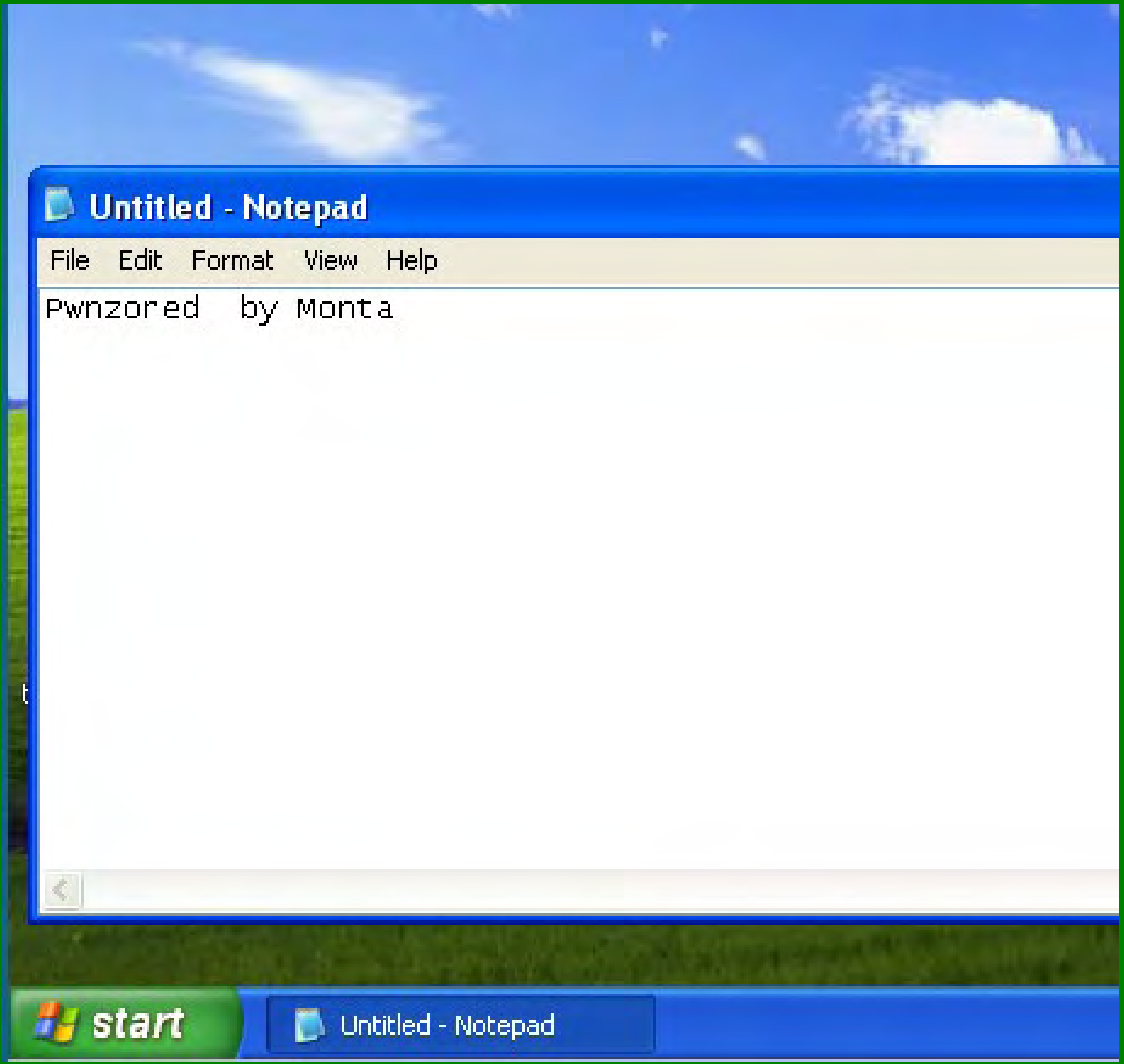


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: notepad.exe

Windows Attack 01 (continued)



Pwnzored by Monta

After opening the notepad.exe window, URFUKED types text into the window in this demonstration "attack"

Inspiration

Inspiration

Inspired by (Adrian Crenshaw) the IronGeek's: Programmable HID USB Keystroke Dongle [PHUKD].

URFUKED overcomes the blind timing, and attack selection difficulties, by incorporating an RF transmitter and expands the concept to include multiple O.S. attacks.

[Adrian, I know you're here somewhere, Thanks! I owe you a beer.]

Interface Details

Using The Interface

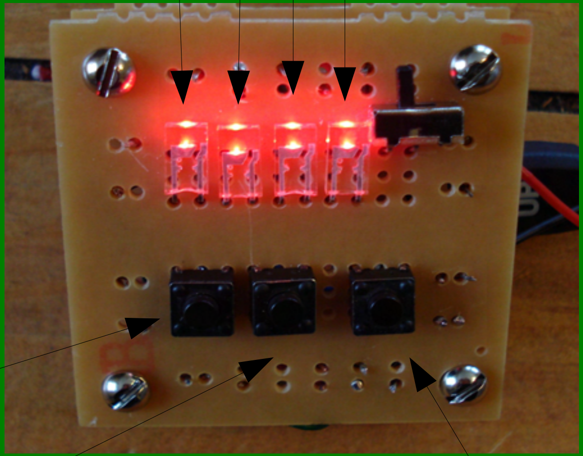
First two lights represent O.S. to attack:

01=Windows
10=Mac
11=Linux
00=Mouse Attack
(for mouse attack the two attack lights represent length of attack)

These two lights represent the attack to perform:

00 = notepad message
01 = web page load
10 = download software
11 = rm -rf

Easily expandable to 64 different attacks.



Enter a “0”

Enter a “1”

Transmit Attack

Transmission Protocol

Transmission Frames

Receiver continually “receives” bytes even when there is no transmission due to ambiant RF noise. I use these frames to distinguish a transmission from noise.

Valid Frame Definition:

- 3 Carrier Bytes (or more)
  - 0xAA
- Command Sequence Number
  - 0-127
- Command Byte
  - Any value
- Checksum
  - Command Sequence Number + Command Byte

Transmission

For reliability the transmitter sends the following command frame 10 times for each command send button press.

- 10 Carrier Bytes
  - 0xAA
- Command Sequence Number
  - 0-127
- Command Byte
  - Any value
- Checksum
  - Command Sequence Number + Command Byte

x 10

Each command frame is repeated 10 times for redundancy- the command is only executed once by the receiver even if multiple valid copies are received due to the Command Sequence Number.

Software

Software Location

http://www.hackerwarrior.com/urfuked

Attack Scenarios

Scenarios

- Exfiltrate information from the target
- Infiltrate (plant) information on target computer
- Install remote administration tool or virus on the target
- Political style attacks
  - Facebook postings
  - In appropriate web browsing (in conjunction with mouse control
- Disabling attacks
  - rm -rf style
  - Remove all files in home directory etc.
- Financial Attacks
  - Paypal transfer attack
  - Ebay bid attack

Modifying Software for Unique Attacks

Key Selection

Sources

Sources

Part	Source	Price
Teensy uc	http://www.pjrc.com/store/teensy.html	$18.00
Transmitter	http://www.hvwtech.com/products_view.a 1042 http://www.sparkfun.com/commerce/product_info.php?products_id=8945	$3.95
Receiver	www.hvwtech.com/products_view.asp?P http://www.sparkfun.com/commerce/product_info.php?products_id=8948	$4.95
Buttons, LED's, misc. Available from a variety of sources	http://www.digikey.com/ http://www.mouser.com/ http://www.radioshack.com	
USB adapter	http://www.dealextreme.com/details.dx/sku.2704~r.48687660	$1.07