PROGRAMMABLE HID USB KEYBOARD/MOUSE DONGLE FOR PEN-TESTING

Adrian Crenshaw

http://Irongeek.com

About Adrian

- I run Irongeek.com
- I have an interest in InfoSec education
- I don’t know everything - I’m just a geek with time on my hands

First, a little story

- I was given a device called a Phantom Keystroker at Shmoocon 2010 for doing a FireSide talk

- Meant to annoy someone by sending keystrokes and mouse movements

- But, what if it was programmable?

Darren and Robin

- Darren Kitchen (media mogul) and Robin Wood (code deity)
- I knew Darren had been working with the U3 thumb drives for automated attacks, so I went to him with the idea
- Devious minds think alike! They were already developing it!
- They are working on a product (USB Rubber Ducky): http://www.hak5.org/store

Darren Kitchen http://hak5.org

Robin Wood
http://digininja.org

Playing with the idea

- If you want something nicer, wait for Darren and Robin's tool
- For those that like to "Go ugly early", hold on for the rest of this presentation
- Three notes in my defense:

1. I'm new to microcontrollers
2. I suck at soldering (Like an epileptic alcoholic with DTs soldering with an aluminum baseball bat)
3. I apparently suck at using rotary tools too

Why would you want a programmable keystroke device?

- Likely types faster than you can, without errors
- Works even if U3 autorun is turned off
- Draws less attention than sitting down in front of the terminal would. The person turns their head for a minute, the pen-tester plugs in their programmable USB key stroke dongle, and Bobs your uncle, instant pwnage.
- Can also be set to go off on a timer when you know a target will be logged in
- Just use your imagination!

What sort of commands would you want to issue?

- Add as user
- Run a program
- Copy files to your thumbdrive
- Go to a website they have a cookie for, and do a sort of CSRF (sic)

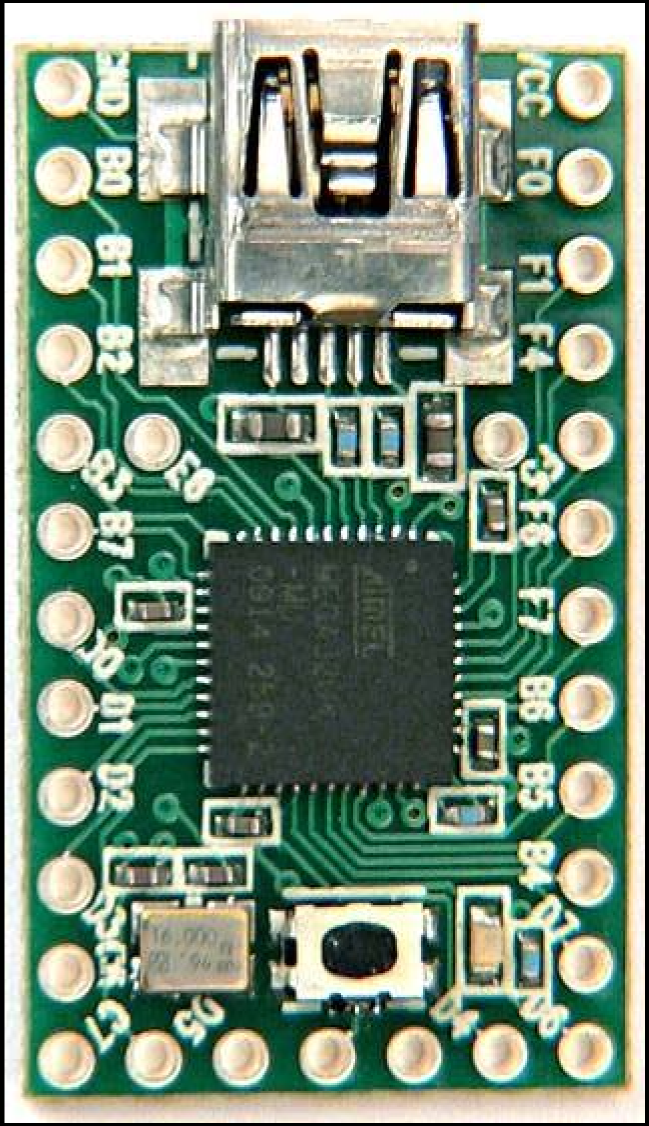
What is in a name?

- MintyPwn?
- DIPStick?
- Programmable Hid USB Keyboard/Mouse Dongle?
- Maybe an acronym? Let’s see:
  Programmable Hid USB Keyboard/Mouse Dongle?
- PHUKD

Ok, we have some names, not how would we build one?

- Did some Googling…
- Found some limited items…
- Then I found…

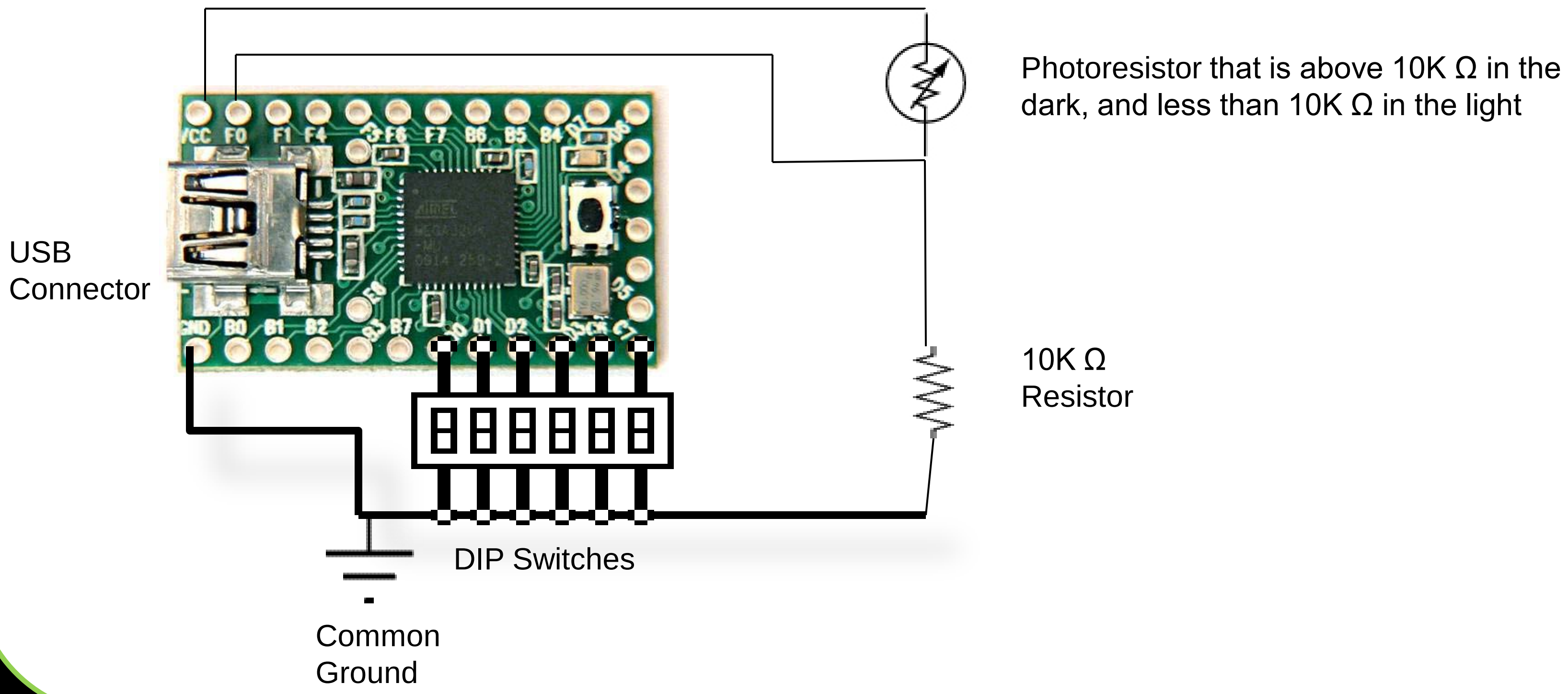
The Teensy



http://Irongeek.com

- ▣ 1.2 by 0.7 inch
- ▣ AVR processor, 16 MHz
- ▣ Programmable over Mini USB in C or Arduino dev package
- ▣ $18 to $27
- ▣ USB HID Support!!!
- ▣ http://www.pjrc.com/teensy/

Butt Ugly Schematic

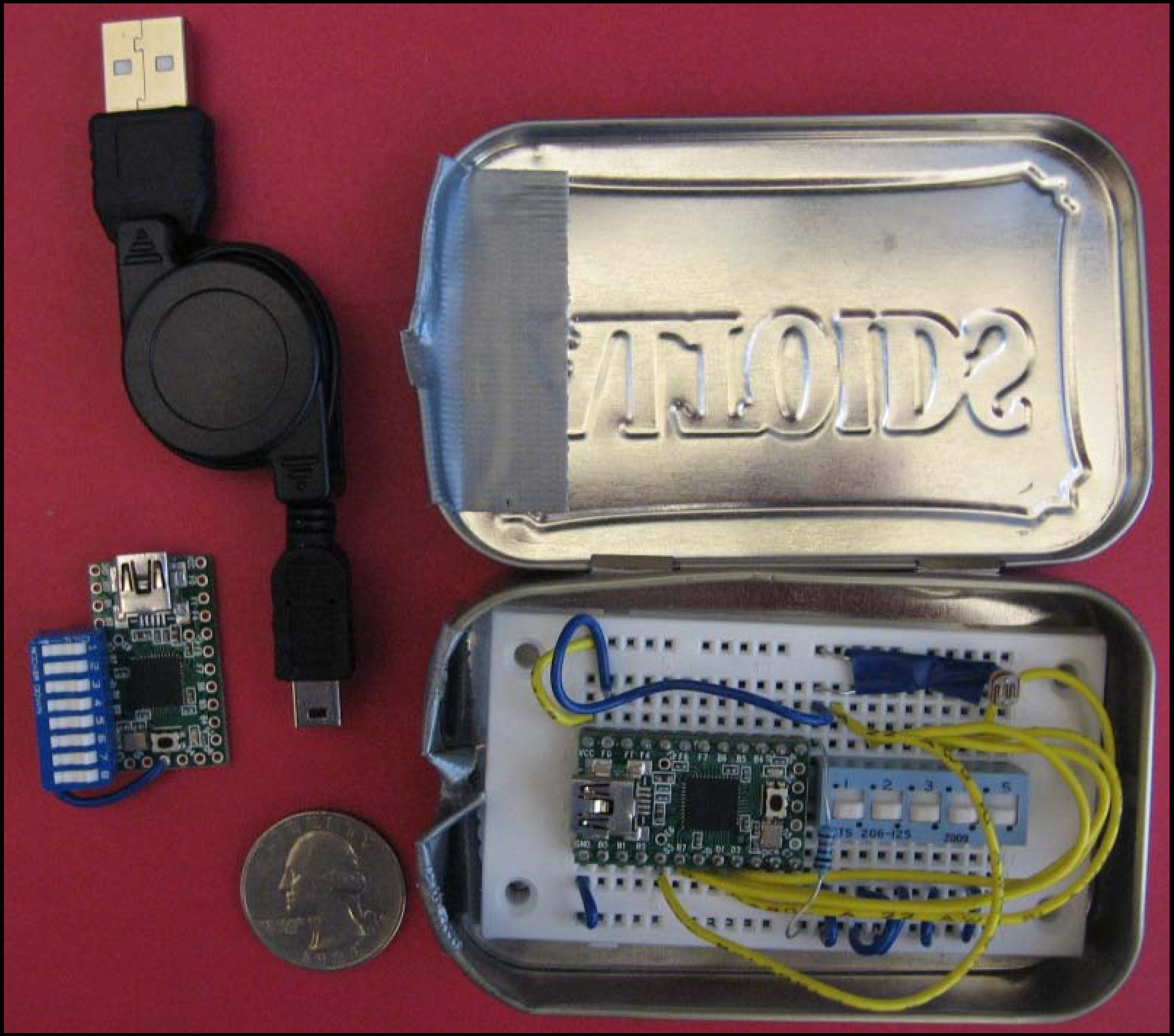

Photoresistor that is above 10K Ω in the dark, and less than 10K Ω in the light
USB Connector
VCC F0 F1 F4 F6 F7 B6 B5 B4
GND B0 B1 B2 B3 B7 D0 D1 D2
10K Ω Resistor
DIP Switches
Common Ground

Please note that the Teensy can use internal pullup resistors

Code Example

```
int ledPin =  11;    // LED connected to digital pin 13
// The setup() method runs once, when the sketch starts
void setup()   {
  // initialize the digital pin as an output:
  pinMode(ledPin, OUTPUT);
  pinMode(PIN_D2, INPUT_PULLUP); // Pushbutton
}
// the loop() method runs over and over again,
// as long as the Arduino has power
void loop()
{
  if (digitalRead(PIN_D2)) {
        digitalWrite(ledPin, LOW);    // set the LED off
  }
  else {
    // Keyboard.set_modifier(MODIFIERKEY_CTRL|MODIFIERKEY_ALT);
    digitalWrite(ledPin, HIGH);   // set the LED on
    Keyboard.set_modifier(128); //Windows key
    Keyboard.set_key1(KEY_R); // use r key
    Keyboard.send_now(); // send strokes
    Keyboard.set_modifier(0); //prep release of  control keys
    Keyboard.set_key1(0); //have to do this to keep it from hitting key multiple times.
    Keyboard.send_now(); //Send the key changes
    delay(1500);
    Keyboard.print("notepad.exe");
    delay(500);
    Keyboard.set_key1(KEY_ENTER);
    Keyboard.send_now();
    Keyboard.set_key1(0);
    Keyboard.send_now();
    delay(1000);
    Keyboard.print("Adrian Was here!!! :)");
    delay(2000);  }
}
```

Device Demo



Other ideas

- ▣ Embed a hub and storage in better packaging http://www.dealextreme.com/details.dx/sku.2704~r.48687660
- ▣ Leave it around in a thumb drive package for unsuspecting people to pick up and use
- ▣ Trojaned Hardware: Use a timer or sensor and embed it in another device you give to the target as a “gift“
- ▣ Have it “wake up”, mount onboard storage, run a program that covers what it is doing (fake BSOD for example), does its thing, then stops (leaving the target to think “it’s just one of those things”)
- ▣ Default BIOs password brute forcing?

Links

Hak5

http://www.hak5.org/store

Teensy Product Page

http://www.pjrc.com/teensy/index.html

Code will be on my site soon

http://www.irongeek.com/

Events

- Free ISSA classes
- ISSA Meeting
  http://issa-kentuckiana.org/
- Louisville Infosec
  http://www.louisvilleinfosec.com/
- Phreaknic/Notacon/Outerz0ne
  http://phreaknic.info
  http://notacon.org/
  http://www.outerz0ne.org/

QUESTIONS?

42