Hardware Hacking Village
Virtual Edition

Intro to Microcontroller Coding:
Making your own HID

By: Mick Douglas

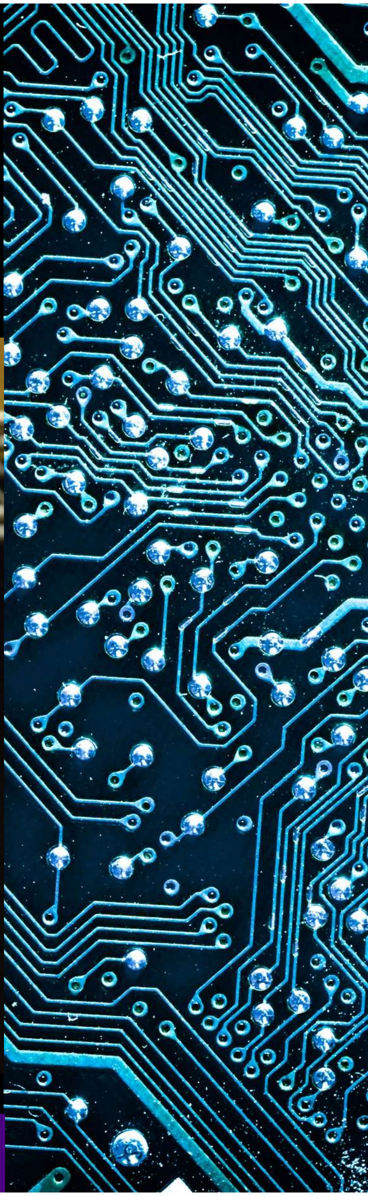
Hardware Hacking is Fun!

- SANS is doing more with Hardware Hacking
- Network Security Las Vegas TV-B-Gone type clones

- Showing you the platform we'll be using for HWHV

About Me

- Managing Partner of InfoSec Innovations
- Teach 504 & 555
- @BetterSafetyNet



About this Talk

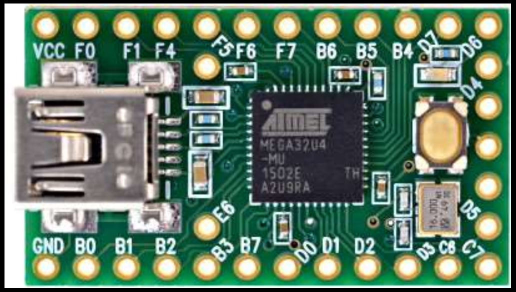
^
We’ll be here today.

Not that “advanced” because… you almost don’t need to be!

USB HIDS

- USB Human Input Device
- Keyboards, mice, presentation clickers, etc.
- And… potentially malicious devices!

Teensy


VCC F0 F1 F4 F5 F6 F7 B6 B5 B4 D7 D6
D4
ATMEL
MEGA32U4
-MU
1502E
A2U9RA
TH
E6
D5
GND B0 B1 B2 B3 B7 D0 D1 D2 D3 C6 C7

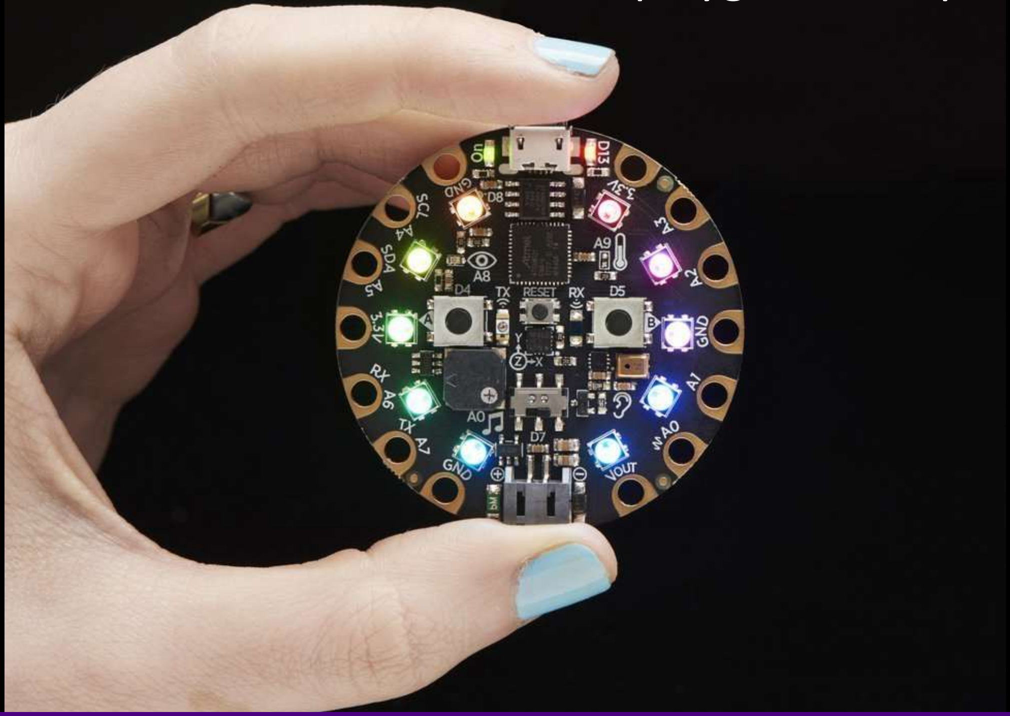
https://www.pjrc.com/store/teensy.html

Rubber Ducky

https://shop.hak5.org/products/usb-rubber-ducky-deluxe

Ada Fruit Industries
Circuit Playground Express

https://learn.adafruit.com/adafruit-circuit-playground-express/overview



And many more…

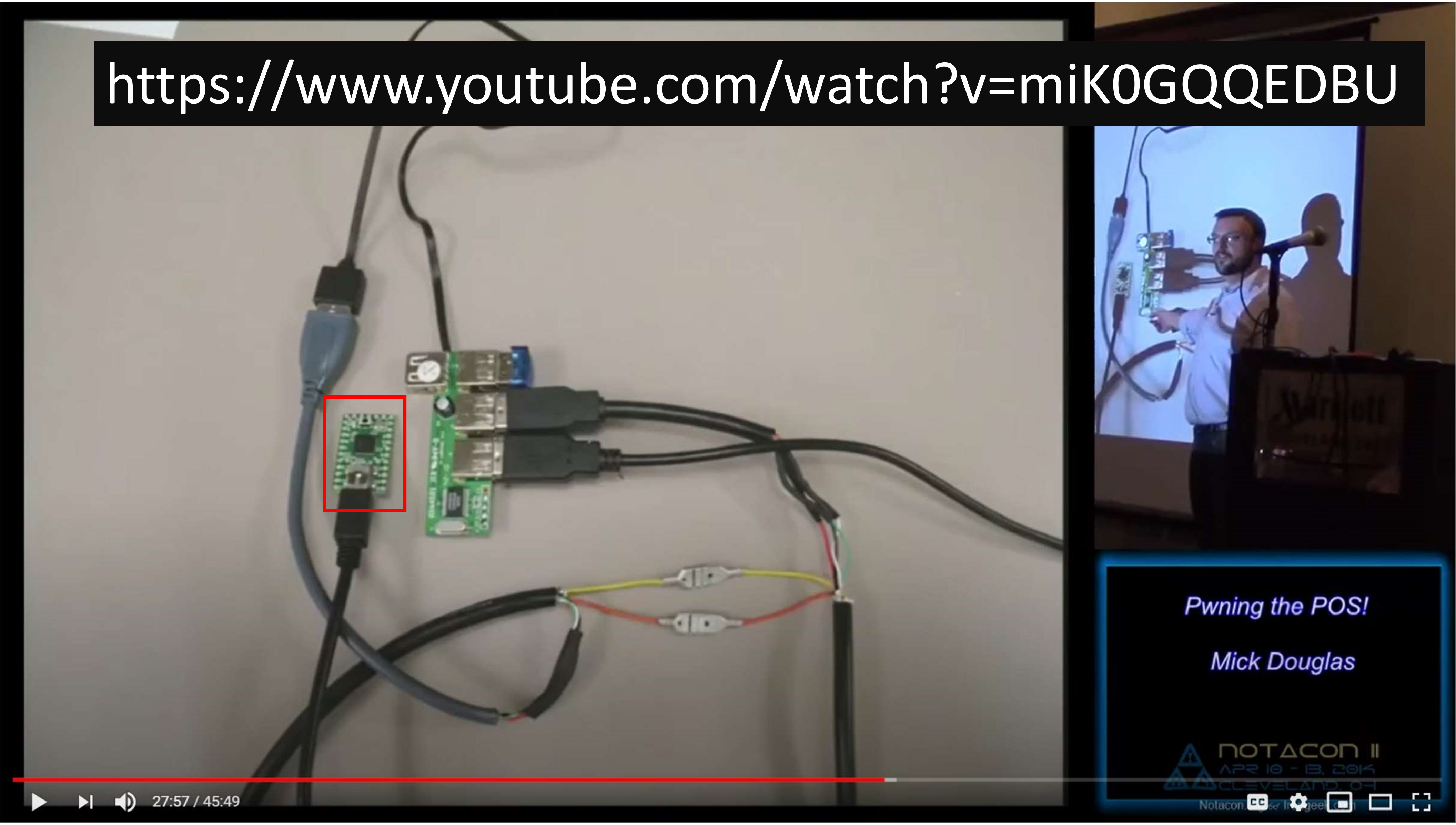
- Specialized
- Drone controllers

- Super small form factor (tinycurcuits.com)

What can you do? It’s just a keyboard, right?

- YOU CAN DO ANYTHING!!!

https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads https://www.youtube.com/watch?v=miK0GQQEDBU



Circuit Playground Express

Cons

Can make debug a bit trickier…

Not too stealthy…

Circuit Playground Express

- PROS

- Fantastic community
- Well documented
- Easy to use all-in-one platform
  (lots of components, cost savings too!)

Circuit Playground Express Components

- 10 RBG LEDs (Neo Pixels)
- 3-axis motion accelerometer
- Thermo-resister (temperature sensor)
- Phototransister (light sensor)
- Mic
- Speaker
- Slide switch
- Two push buttons

A lab in the palm of your hand!

Shipping is much slower now…

Airlines hit the pause button

Grounded Lufthansa planes at Frankfurt Airport on March 15.

Frank Rumpenhorst/picture alliance via Getty Images

Programing the device

- Various bit of software to help make this work
- Strongly suggest Arduino IDE or Python editor like Mu

Setting up is easy as 1. 2. 3!

1. Setup Mu-Editor
   (be sure to set mode!)

Setting up is easy as 1. 2. 3!

2. Update your Circuit Boot loader

Trickiest bit… double pressing the reset button…

(download latest library code, and copy to device)

Setting up is easy as 1. 2. 3!

3. Get coding!

Wait that’s… it?

Seems rather “basic”… because it is…

Ponder this, if you had keyboard access…

you pretty much own that machine!

Cautions… nothing's perfect…

Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a ogramable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID

Cautions… nothing's perfect…

Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a ogramable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID
Hi my name is Mick Douglas! I cannot wait to show you the fun you can have with a programable HID

Dealing with data problems

- Test!
- May need to have checks… ping, nc, other “call backs”

Cautions… Virtualization

Some issues with virtualized systems…

Makes for something else to troubleshoot.

Recommend that you setup on physical systems where you can.

Defending against these attacks

- Baselines to the rescue!
- Super easy… these are ***NOT*** stealthy

```
Get-CimInstance -ClassName Win32_PnPDevice | Measure-Object -Line
```

Questions?

Closing

- Microcontrollers are fun
- Easier than PIC or STAMP chips
- AdaFruit Circuit playground is one of the easiest entry points!
- Try these… they work well on pen tests with physical access.
- Detecting these is dead easy… but you have to look!

Thanks

- SANS and the Hackfest Committee
- AdaFruit Industries
- Larry & Micah